Univerzita Palackého v Olomouci
Právnická fakulta

Nicole Firlová

Právní aspekty používání bezpečnostních kamer bytovými domy

Diplomová práce

Olomouc 2020

Prohlašuji, že jsem diplomovou práci na téma *Právní aspekty používání bezpečnostních kamer bytovými domy* vypracovala samostatně a citovala veškeré použité zdroje.

V Bruntále dne 27. 7. 2020

……

Nicole Firlová

Touto cestou bych ráda poděkovala Mgr. Petře Melotíkové, Ph.D. za odborné vedení, vstřícnost, trpělivost a cenné rady a připomínky, které mi při psaní této diplomové práce poskytovala.

Obsah

Seznam použitých zkratek

GDPR/Obecné nařízení	Obecné nařízení o ochraně osobních údajů
NSS	Nejvyšší správní soud
Úřad	Úřad pro ochranu osobních údajů
ESLP	Evropský soud pro lidská práva
EU	Evropská Unie
EDPB	European Data Protection Board
SVJ	Společenství vlastníků jednotek
OECD	Organizace pro hospodářskou spolupráci a rozvoj
Listina	Listina základních práv a svobod
Úmluva	Evropská úmluva o ochraně lidských práv
zákon o ochraně osobních údajů	Zákon č. 101/2000 Sb., o ochraně osobních údajů
zákon o zpracování osobních údajů	Zákon č. 110/2019 Sb., o zpracování os. údajů
občanský zákoník	Zákon č. 89/2012 Sb., občanský zákoník
zákon o obchodních korporacích	Zákon č. 90/2012 Sb., o obchodních korporacích
soudní řád správní	Zákon č. 150/2002 Sb., soudní řád správní
správní řád	Zákon č. 500/2004 Sb., správní řád
FO	Fyzická osoba
PO	Právnická osoba

Úvod

Používání bezpečnostních kamer soukromými osobami je v dnešní době běžnou záležitostí. Spousta nejen rodinných domů, ale i bytových domů zavádí bezpečnostní kamery. Činí tak nejčastěji za účelem ochrany svého majetku a dále ochrany života a zdraví nejen sebe, ale i ostatních rodinných příslušníků. Ne vždy jsou však dodržovány všechny podmínky spojené s instalací a provozem bezpečnostní kamery.

Český právní řád nedisponuje zákonem, který by tuto problematiku jako celek upravoval. Nápomocným v této oblasti je Úřad pro ochranu osobních údajů, který vydává nejrůznější stanoviska nejen ve vztahu k ochraně osobních údajů obecně, ale i k problematice bezpečnostních kamer, kterými se tato práce bude zabývat. Několik sporných otázek se podařilo vyřešit i díky bohaté judikatuře Nejvyššího správního soudu. Lze nalézt také odbornou literaturu, která se věnuje přímo problematice bezpečnostních kamer. I přesto však existuje řada nezodpovězených či sporných otázek, zejména pak po přijetí evropského právního předpisu známého pod zkratkou GDPR.

Používání bezpečnostních kamer souvisí se zpracováním osobních údajů. Odborná literatura se hojně zabývá problematikou ochrany osobních údajů. Jak jsem již ale zmínila, otázce ochrany osobních údajů konkrétně při pořizování kamerových záznamů již tolik pozornosti věnováno není. Proto jsem zvolila výzkumnou otázku: *jakým způsobem je zabezpečena ochrana osobních údajů získaných z kamerových záznamů konkrétních subjektů?* Na tuto výzkumnou otázku navazuje další, a sice *zda je ochrana osobních údajů při pořizování kamerových záznamů poskytována dostatečně?* V průběhu psaní této práce nepochybně vyvstanou další otázky, na které bude třeba odpovědět. Jako hlavní cíl mé diplomové práce jsem si poté stanovila analyzovat podmínky pro používání bezpečnostních kamer a zhodnotit na kolik se potvrdila má hypotéza, že *provoz bezpečnostních kamer je doprovázen množstvím podmínek, jejichž naplnění je nutné pro to, aby získané osobní údaje byly dostatečně chráněny*.

Tato diplomová práce je rozčleněna do šesti kapitol. Nejdříve se zaměřím na právní úpravu ochrany osobních údajů a vymezení základních pojmů v souvislosti s ochranou osobních údajů. Při psaní této kapitoly budu využívat metodu deskripce.

V následujících částech této práce se budu zabývat otázkou pořizování kamerového záznamu, tedy vůbec těmi základními otázkami spojenými s pořizováním záznamu, na které je potřeba si odpovědět dříve, než se přistoupí k zavedení kamerového systému. Poté se zaměřím na konkrétnější otázky, jako jsou prostory kamerově sledované, souhlas se zpracováním osobních údajů jako jeden z nejčastějších a zároveň nejdiskutovanějších zákonných titulů pro

zpracování osobních údajů. Dále se zaměřím také na to, jak má konkrétní subjekt nakládat s kamerovým záznamem. V těchto zmíněných částech budu využívat zejména metodu analýzy, z části pak také metodu deskripce.

V šesté části práce pomocí metody komparace srovnám stav před přijetím GDPR a po něm, kdy uvedu z mého pohledu nejdůležitější změny, které Obecné nařízení přineslo.

Závěrem vyhodnotím poznatky, které jsem při psaní této práce získala, a to za použití metody syntézy, indukce a dedukce. V této části tak odpovím na zvolené výzkumné otázky a na případné další otázky, které v průběhu psaní této práce vyvstaly.

Stěžejním zdrojem této práce bude komentářová literatura k Obecnému nařízení, tedy komentář Pattynové a komentář Nulíčka. Dále práce bude čerpat poznatky z publikací například od Janečkové, Bartíka, Žůrka a dalších. Dále budu pracovat s právními předpisy a judikaturou Nejvyššího správního soudu, která je na toto téma poměrně bohatá. Opomenuty nebudou ani stanoviska Úřadu pro ochranu osobních údajů reagující jednak na vývoj judikatury, ale i změny v právní úpravě týkající se ochrany osobních údajů obecně.

Tato práce vychází z právního stavu ke dni 27. 7. 2020.

1 Základní aspekty ochrany osobních údajů

U provozování bezpečnostních kamer je důležité si uvědomit, že tato činnost souvisí se zpracováním osobních údajů. Právní úprava, o kterou se provoz bezpečnostních kamer opírá, se týká ochrany osobních údajů. V dnešní době, kdy žijeme ve světě digitálních technologií je třeba lpět na ochraně osobních údajů. Život jednotlivce v současné době provází různé vymoženosti moderních technologií, osobní údaje jsou tak zpracovávány prakticky denně. Co se týče konkrétně kamerových systémů, ty lze dnes označit za novodobou zbraň, jelikož mohou výrazně ohrozit právem chráněný zájem, a to soukromí člověka. Pokud budou kamerové systémy nesprávně provozovány, může se osoba provozující takový kamerový systém velmi snadnou ocitnout na druhé straně zákona. Kamerové systémy jsou v tom nejširším slova smyslu neoddělitelně spjaty s ochranou soukromí. Zároveň zahrnují zpracování osobních údajů.[1] Jelikož jsou tedy schopny poměrně citelně zasáhnout do práv a svobod jednotlivců, považuji za nezbytné uvést právní úpravu dopadající na pole ochrany osobních údajů a zároveň uvést a charakterizovat základní pojmy související s osobními údaji.

1.1 Právní úprava

1.1.1 Právní úprava na mezinárodní úrovni

V rovině mezinárodní budou pramenem práva mezinárodní smlouvy, které jsou na základě čl. 10 ústavního zákona č. 1/1993Sb., Ústavy České republiky součástí právního řádu. Musí se však jednat o takové smlouvy, které byly vyhlášeny, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána. Zároveň je zde aplikační přednost těchto mezinárodních smluv. Součástí právního řádu jsou i mezinárodní smlouvy upravující základní lidská práva a svobody. Ústava tak sice výslovně nestanoví, nicméně Ústavní soud k tomuto přijal jednoznačný závěr, že součástí ústavního pořádku jsou i ratifikované a vyhlášené mezinárodní smlouvy o lidských právech.[2]

Prvně je třeba zmínit Mezinárodní pakt o občanských a politických právech, který v čl. 17 zakazuje svévolné zasahování do soukromého života a přiznává každému právo na zákonnou ochranu proti neoprávněným zásahům do soukromého života.

Na regionální (evropské) úrovni je třeba zmínit Úmluvu o ochraně lidských práv a základních svobod. Tato Úmluva v čl. 8 upravuje právo na respektování soukromého života a

[1] ŽŮREK Jiří. *Praktický průvodce GDPR*. 2. vydání. Olomouc: Anag, 2018. s. 215
[2] SLÁDEČEK, Vladimír a kol. *Ústava České republiky, Komentář*. 2. vydání. Praha: C. H. Beck, 2016. 1264 s. (čl. 10)

zakazuje státním orgánům do tohoto práva zasahovat, vyjma případů, kdy takový zásah bude v souladu se zákonem a zároveň bude nezbytný v demokratické společnosti. Rovněž i Evropský soud pro lidská práva má v oblasti ochrany soukromí bohatou judikaturu, která nejenže vykládá tato ustanovení Úmluvy, ale zároveň tímto nastavuje i jistá pravidla v rámci ochrany soukromí na území Evropy.

Za zmínku stojí i Úmluva č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních údajů jakožto právní předpis navazující na již zmíněný čl. 8 Úmluvy o ochraně lidských práv a základních svobod.

1.1.2 Právní úprava Evropské unie

Evropská unie má také svou úpravu práva na soukromí a ochrany osobních údajů, a to na úrovni primárního i sekundárního práva. Smlouva o Evropské unii v čl. 6 odst. 3 zakotvuje ochranu základních práv zaručených Úmluvou o ochraně lidských práv a základních svobod. Evropské právo se tímto přihlásilo k aplikaci základních práv a svobod zaručených již v Úmluvě, tedy i práva na ochranu soukromí zaručeného v čl. 8 Úmluvy. Smlouva o Evropské Unii v čl. 6 odst. 1 stanoví, že EU uznává práva, svobody a zásady, které jsou obsaženy v Listině základních práv EU. Listina základních práv EU samozřejmě neopomenula ochranu osobních údajů a v čl. 7 deklaruje právo na respektování soukromého života. V následujícím čl. 8 pak deklaruje právo na ochranu osobních údajů. Lze tedy uzavřít, že Listina základních práv EU výslovně zakotvuje ochranu osobních údajů jakožto základní právo.[3]

V rámci primárního práva nelze opomenout ani Smlouvu o fungování Evropské Unie, která v čl. 16 upravuje právo na ochranu osobních údajů a dále opravňuje Evropský parlament a Radu k přijetí pravidel ohledně zpracovávání osobních údajů. Tohoto oprávnění bylo ze strany Evropského parlamentu i Rady využito, když bylo vydáno nařízení (ES) 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů.

Z oblasti sekundárního práva lze dále zmínit například nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikací).

Právní rámec ochrany osobních údajů na evropské úrovni je v současné době tvořen Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně

[3] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světe: Komentář*. Praha: Leges, 2018, s. 23 – 26 (čl. 1 GDPR)

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). Pro Obecné nařízení jakožto stěžejní právní předpis na poli ochrany osobních údajů je používána anglická zkratka GDPR (General Data Protection Regulation). Tomuto právnímu předpisu se budu více věnovat ještě v pozdější podkapitole.

1.1.3 Právní úprava na národní úrovni

V případě národní právní úpravy, nelze opomenout Listinu základních práv a svobod. Listina v čl. 7 zaručuje nedotknutelnost osoby a jejího soukromí. V čl. 10 odst. 2 Listiny je pak poskytnuta ochrana před neoprávněným zasahováním do soukromého a rodinného života. Čl. 13 Listiny poskytuje ochranu listovnímu tajemství a jiných písemností a záznamů.

V rovině běžných zákonů je třeba uvést zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, který v § 81 a násl. upravuje ochranu osobnosti a v případě zásahu do osobnostních práv pak tento zákon umožňuje domáhat se náhrady škody ve smyslu § 2956 a následujících.

V neposlední řadě lze odkázat také na zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, který v § 180 a násl. upravuje trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství.

V předchozí podkapitole jsem zmínila hlavní pramen právní úpravy ochrany osobních údajů, a to GDPR. Dříve než se Česká republika začala řídit GDPR, byl na národní úrovni klíčovým právním předpisem zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Zákonodárce však musel reagovat na změny, které nastaly v důsledku GDPR, a proto byla na národní úrovni přijata nová právní úprava, a sice zákon č. 110/2019 Sb., o zpracování osobních údajů. Tento zákon nabyl platnosti a účinnosti dne 24. dubna 2019 a zrušil dosud platný a účinný zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. [4]

1.1.4 Obecné nařízení o ochraně osobních údajů

Jedním z klíčových právních předpisů, který bude podkladem této diplomové práce je již zmíněné Obecné nařízení o ochraně osobních údajů, zkráceně označováno jako GDPR nebo Obecné nařízení. Jelikož se jedná o hlavní pramen právní úpravy na poli ochrany osobních údajů, rozhodla jsem se mu věnovat samostatnou podkapitolu. GDPR nahradilo dosud platnou

[4] zákon č. 110/2019 Sb., o zpracování osobních údajů, § 67

úpravu na poli ochrany osobních údajů a sice směrnici č. 95/46/EC (Data Protection Directive). GDPR zavádí několik nových práv pro subjekty údajů (např. právo být zapomenut), ale také nové povinnosti (např. oznamování porušení zabezpečení či osobu pověřence).[5]

Ve vztahu k Obecnému nařízení se hovoří o jeho přímém účinku. Přímý účinek byl zakotven Soudním dvorem EU v případu Van Gend en Loss[6]. V tomto rozhodnutí soud uvedl, že i jednotlivci se mohou dovolávat práv zakotvených evropským právem. Rozlišuje se vertikální přímý účinek ve vztazích mezi jednotlivci a příslušným státem a horizontální účinek ve vztazích mezi jednotlivci navzájem. Předpokladem přímého účinku unijní normy je její přímá použitelnost. Norma unijního práva je přímo použitelná, pokud může přímo zakládat práva či povinnosti jednotlivci. Tomu tak bude tehdy, pokud norma bude dostatečně jasná, aby z ní bylo možné dovodit právo nebo povinnost jednotlivce. Dále musí být příslušná norma bezpodmínečná, tedy nesmí být závislá na splnění podmínky dle jiného ustanovení ať už unijního, či vnitrostátního práva a zároveň nesmí ponechávat členským státům prostor pro legislativní upřesnění takového normy. Tyto podmínky byly postupem času Soudním dvorem EU v případu Defrenne[7] zmírněny. Podmínka jasnosti je naplněna i v případě, že danou normu lze jasně a konkrétně interpretovat. Dokonce i v případě, kdy vnitrostátnímu zákonodárci uplyne lhůta pro upravení dané otázky, můžeme následně hovořit o přímém účinku.[8]

V současnosti je přímá použitelnost nařízení zakotvena v čl. 288 Smlouvy o fungování EU a není tak vyžadována implementace ze strany členského státu. Nařízení má také aplikační přednost před právními předpisy členských států. To znamená, že v případě rozporu některého ustanovení vnitrostátního předpisu s Obecným nařízením, bude aplikováno ustanovení Obecného nařízení. Dále není možné, aby stát zavedl přísnější podmínky pro ochranu osobních údajů, než stanoví Obecné nařízení, ledaže by toto výslovně připouštělo. [9]

Pokud se vrátíme k samotnému GDPR jako takovému, je potřeba vymezit si věcnou a místní působnost tohoto nařízení. Článek 2 Obecného nařízení stanoví věcnou působnost, tedy případy zpracování osobních údajů, na které GDPR dopadá. Jedná se o automatizované zpracování osobních údajů a neautomatizované zpracování takových osobních údajů, které jsou obsaženy v evidenci nebo ty které mají být do evidence zařazeny.

---

[5] CUSTERS, Bart and others. *EU Personal Data Protection in Policy and Practise*. The Netherlands: T.M. C. Asser Press, 2019. 249 s.
[6] Rozsudek ze dne 5. února 1963, Van Gend en Loss , C 26/62
[7] Rozsudek ze dne 8. dubna 1976, *Defrenne v Sabena, C* 47/75
[8] TOMÁŠEK, Michal a kol. *Právo Evropské unie.* Praha: Leges, 2013. s. 65 – 70
[9] NULÍČEK, Michal a kol. *GDPR/Obecné nařízení o ochraně osobních údajů: Komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018. (čl. 1 GDPR)

Dále článek 2 Obecného nařízení uvádí i případy zpracování osobních údajů, které pod regulaci GDPR nespadají. Do negativního výčtu případů zpracování osobních údajů patří mimo jiné i zpracování osobních údajů prováděné fyzickou osobou v průběhu výlučně osobních či domácích činností.[10] Jedná se o případy, kdy si daná fyzická osoba sbírá fotografie do rodinného alba nebo když si vede adresář se jmény a kontakty dalších osob. Pokud takto osoba činí výlučně pro svou osobní či domácí potřebu, nebude spadat pod regulaci GDPR. Opačná situace by nastala tehdy, kdyby daná fyzická osoba využila svůj adresář pro komerční účely. V případě, že se jedná o provozování bezpečnostní kamery za účelem ochrany svého majetku, je důležité, co všechno kamera zachycuje. V případě, že fyzická osoba provozuje bezpečnostní kameru na vlastním pozemku, lze říci, že se jedná o zpracování především pro osobní potřebu. Jestliže však bezpečnostní kamera zachycuje i veřejné prostranství nebo sousedův pozemek, pak už se nejedná výlučně o zpracování osobních údajů pro osobní potřebu a výjimka z působnosti GDPR se neuplatní. Závěrem je potřeba říci, že požadavek osobní potřeby se nemusí vztahovat výlučně k osobě provádějící zpracování. Je přípustná i situace, kdy daná osoba bude také sledovat zájmy svých rodinných příslušníků, členů domácností nebo osob blízkých. V takových případech se bude stále jednat o zpracování osobních údajů pro osobní potřebu a takovéto situace budou z působnosti GDPR vyňaty.[11] Více bude tato problematika vymezena v dalších částech této práce.

Místní působnost nařízení je upravena v čl. 3 Obecného nařízení. K aplikaci Obecného nařízení dojde ve třech případech. Prvně půjde o případy, kdy zpracování osobních údajů bude probíhat v souvislosti s činností provozovny správce nebo zpracovatele nacházejících se na území EU. Druhým případem budou situace, kdy správce i zpracovatel budou mimo EU, ale budou zpracovávat osobní údaje subjektů, kteří se naopak v EU nachází. Třetím případem aplikace Obecného nařízení jsou situace, kdy se na základě mezinárodního práva veřejného aplikuje právní řád členského státu.[12]

1.2 Vymezení základních pojmů

Tato diplomová práce bude pracovat s několika klíčovými pojmy. Jedná se o pojem osobní údaj, zpracování, správce, zpracovatel a dozorový úřad. Jelikož bude s těmito pojmy pracováno poměrně často, považuji za vhodné je nejdříve charakterizovat.

[10] čl. 2 odst. 2 písm. c) GDPR
[11] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR)…,* s. 36 – 38 (čl. 2 GDPR)
[12] NULÍČEK, Michal a kol. *GDPR/Obecné nařízení o ochraně osobních údajů…*, s. 69 (čl. 3 GDPR)

1.2.1 Osobní údaj

Z hlediska ochrany osobních údajů je nezbytné vymezit pojem osobní údaj. GDPR vymezuje osobní údaje jako „*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, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby*.“[13]

Zjednodušeně můžeme říci, že osobním údajem je každý údaj vztahující se k nějaké fyzické osobě. Ve chvíli, kdy bude údaj přiřazen k fyzické osobě, stává se osobním údajem.[14]

Osobní údaj byl vůbec poprvé definován OECD v Pravidlech ochrany soukromí a přeshraničních toků osobních údajů v roce 1980. Tento dokument však postrádal obecnou závaznost a byl vydán pouze jako doporučení pro členské státy OECD. Cílem vydání těchto Pravidel bylo dosáhnout rovnováhy mezi ochranou soukromí fyzických osob a volným obchodem, tak aby nedocházelo k omezení volného pohybu dat přes národní hranice. Chráněny byly ty údaje, které by v případě jejich zpracování představovaly nebezpečí pro soukromí a svobody jednotlivce.[15]

Co se týče vnitrostátní úpravy, definici obsahoval i zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a to ve svém § 4. Tento zákon byl nahrazen pozdějším zákonem č. 110/2019 Sb., o zpracování osobních údajů. Nová právní úprava již pojem osobní údaj nedefinuje, a tak se vychází z definice obsažené v Obecném nařízení.

V současnosti pod pojmem osobní údaj musíme chápat jakoukoliv informaci týkající se určené nebo určitelné fyzické osoby. Může se jednat i o takové informace, které dotyčného jedince přímo neidentifikují, například počet dětí, dosažené vzdělání nebo zůstatek na bankovním účtu. Takovéto informace ani nemusí být pravdivé, mohou být i pouhým odhadem charakteristiky člověka (například otázka spolehlivosti věřitele). Nerozhoduje ani to, v jaké formě je daná informace zachycena, zda písemně, na audiozáznamu či videozáznamu. Klíčový je naopak vztah příslušné informace ke konkrétnímu jedinci. Obecné nařízení hovoří o identifikované nebo identifikovatelné fyzické osobě. Identifikovat lze fyzickou osobu tehdy, pokud jsou dostupné takové informace o této osobě, díky kterým lze tuto osobu přímo odlišit

[13] čl. 4 bod 1 GDPR
[14] MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana.* 2. vydání. Praha: ASPI, 2008. s 19.
[15] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR)…*, s. 27 (čl. 1 GDPR)

od ostatních osob. Jaké množství informací je potřeba k identifikaci jedince, záleží na konkrétním případu. Identifikovatelná fyzická osoba, tedy určitelná fyzická osoba, je taková osoba, kterou lze identifikovat, a to i za využití dalších údajů, ať už veřejně dostupných nebo zjistitelných od jiných subjektů.[16]

Dále je třeba zdůraznit, že Obecné nařízení pojem osobní údaj přisuzuje pouze fyzické osobě, naopak právnické osoby pod regulaci GDPR nespadají. Nicméně toto neplatí vždy. I některé údaje vztahující se k právnické osobě mohou být osobními údaji. Tak tomu bude v případě, kdy dané údaje budou identifkovat nejen právnickou osobu, ale zároveň i fyzickou osobu. Příkladem mohou být údaje týkající se členů orgánu společnosti.[17]

Na druhou stranu však taková ochrana dobrého jména právnické osoby už do působnosti Obecného nařízení spadat nebude. Je tedy potřeba, aby se daný údaj nějakým způsobem dotýkal fyzické osoby. Bod 26 odůvodnění Obecného nařízení rovněž vylučuje z působnosti nařízení anonymní údaje. Jedná se o takové údaje, které se nevztahují k identifikované či identifikovatelné fyzické osobě a dále informace natolik anonymizované, že daný jedinec není nebo už přestal být identifikovatelným. V prvním případě jde o údaje, které nikdy ani osobními údaji nebyly. V druhém případě jde o údaje, které se dříve daly přiřadit ke konkrétnímu jedinci, avšak v důsledku anonymizace to již nelze.[18]

Závěrem je třeba pamatovat na to, že právní úprava ochrany osobních údajů má za cíl přispět k ochraně soukromí dotčených osob. Z tohoto důvodu by i zcela bagatelní dopad do soukromí dotčené osoby měl být jistým limitem při zvažování, zda určitý údaj je nebo není osobním údajem.[19]

1.2.2 Zpracování

Zpracování definuje Obecné nařízení v čl. 4 bodu 2 jako operaci nebo soubor operací, které jsou prováděny s osobními údaji za určitým cílem bez ohledu na prostředky a způsob zpracování. Je tedy nerozhodné, jak jsou údaje zpracovávány, zda elektronicky či manuálně. Uvedené ustanovení poskytuje demonstrativní výčet operací, které jsou zpracováním osobních údajů. Jedná se například o shromáždění údajů, zaznamenávání, ukládání, vyhledání, použití nebo třeba šíření osobních údajů.

[16] NULÍČEK, Michal a kol. *GDPR/Obecné nařízení o ochraně osobních údajů…*, s. 77 - 84 (čl. 4 GDPR)
[17] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR)…*, s. 53 (čl. 4 bod 1 GDPR)
[18] NULÍČEK, Michal a kol. *GDPR/Obecné nařízení o ochraně osobních údajů…*, s. 81 (čl. 4 GDPR)
[19] Tamtéž

Osobní údaje jsou zpracovávány za účelem dosažení jistého cíle. Tento cíl si buď správce stanoví sám, nebo tak činí proto, že mu to ukládá zvláštní zákon. Nicméně zpracováním ve smyslu Obecného nařízení není každý přístup k datům. Důležitým hlediskem, kdy se bude jednat o zpracování osobních údajů a kdy nikoliv, je již zmiňovaný účel dané činnosti. V případě, že účelem práce bude přístup k údajům jako takovým, bude se jednat o zpracování ve smyslu Obecného nařízení. Příkladem může být uchovávání dat či jejich anonymizace nebo likvidace. Na druhou stranu, pokud bude přístup k údajům jen nahodilý a nepravidelný a bude důsledkem jiné činnosti, už se o zpracování ve smyslu GDPR jednat nebude. Například půjde o situace, kdy bude poskytován nějaký servis či oprava technických prostředků.[20]

1.2.3 Správce

Obecné nařízení dále pracuje s pojmem správce. Definuje jej jako fyzickou či právnickou osobu, orgán veřejné moci, agenturu či jiný subjekt, který buďto sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.[21]

Správcem tak může být osoba soukromého či veřejného práva. Nezáleží ani na právní formě této osoby. Jde především o to, že tato osoba sama nebo společně s jinými subjekty určuje účely a prostředky zpracování. Rozhodování o technických či organizačních věcech týkajících se prostředků zpracování může správce delegovat na jiný subjekt, odpovědnost však i nadále zůstává správci. Byť by tedy správce některé úkoly delegoval na někoho jiného, odpovědnosti se tím nezprostí.[22]

1.2.4 Institut společného správce

Správce může určovat účely a prostředky zpracování sám nebo společně s jiným správcem. Pokud tak budou činit dva či více správců, půjde o společné správce. Obecné nařízení upravuje tento institut v čl. 26. Aby se skutečně jednalo o společné správce, musí se všechny subjekty nacházet v postavení správce a rozhodovat o zásadních věcech (například cíl zpracování či rozsah zpracovávaných údajů). O společné správce tak nepůjde v případě, kdy správce přenechá rozhodování o technických věcech zpracovateli. Zpracovatel totiž nemůže rozhodovat o zásadních věcech týkajících se nakládání s osobními údaji. Z ustanovení čl. 26 GDPR vyplývá, že podíl odpovědnosti za plnění povinností správců nemusí být stejný. Obecné nařízení ponechává na správcích, jak si tuto odpovědnost mezi sebou rozdělí, pokud tato nebude určena

[20] NULÍČEK, Michal a kol. *GDPR/Obecné nařízení o ochraně osobních údajů*…, s. 84 – 86 (čl. 3 GDPR)
[21] čl. 4 bod 7 GDPR
[22] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR)…,* s. 55 (čl. 4 bod 7)

právem Unie nebo členským státem. Ve vztahu k subjektům údajů a odpovědnosti společných správců je potřeba zmínit i skutečnost, že každý ze společných správců má povinnost postupovat při vyřizování žádosti o výkon práv subjektů samostatně a v plném rozsahu. Každý správce tak za vzniklou škodu odpovídá v plné míře, a to bez ohledu na ujednání mezi společnými správci. To znamená, že i pokud si společní správci mezi sebou míru odpovědnosti nějakým způsobem rozdělí, navenek vůči subjektům údajů bude každý z nich odpovídat v plné míře. V rámci vnitřních vztahů se pak společní správci mohou mezi sebou vypořádat s odkazem na ujednání obsažená v dohodě o rozdělení podílu každého z nich na odpovědnosti za plnění povinností.[23]

1.2.5 Zpracovatel

Osobu zpracovatele upravuje nařízení dosti široce, když uvádí, že jím může být fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt zpracovávající osobní údaje pro správce.[24] Z uvedené definice je zřejmé, že zpracovatelem může být prakticky kdokoliv. Osobu zpracovatele dále upravuje i zákon č. 110/2019 Sb., o zpracování osobních údajů, a to v § 34. Uvedené ustanovení upravuje dvě možnosti, jak určit osobu zpracovatele. Pověření zpracovatele vyplývá buď z právního předpisu, nebo na základě písemné smlouvy mezi spravujícím orgánem a zpracovatelem. Příkladem, kdy je konkrétní orgán v postavení zpracovatele osobních údajů na základě výslovného zákonného zmocnění, je Katastrální úřad.[25]

S ohledem na znění čl.4 bodu 8 a čl. 28 Obecného nařízení a dále na dikci ustanovení § 35 zákona o zpracování osobních údajů nelze opomenout skutečnost, že zpracovatel provádí zpracování údajů pro správce. Osoba správce a osoba zpracovatele jsou tedy dvě odlišné osoby.

1.2.6 Dozorový úřad

Obecné nařízení v čl. 4 bodu 21) pamatuje i na dozorový úřad jakožto nezávislý orgán veřejné moci, který členský stát zřídil. Podrobněji je dozorový úřad upraven v čl. 51 a dále Obecného nařízení. GDPR předpokládá, že každý členský stát zřídí alespoň jeden dozorový úřad, který bude dohlížet na uplatňování této evropské legislativy. Důležitou vlastností je nezávislost tohoto dozorového úřadu projevující se ve třech rovinách. Jedná se o nezávislost funkční spočívající v nezávislosti fungování tohoto úřadu na jiných institucích. Dále nezávislost materiální, kdy úřad má být vybaven technickými, finančními a lidskými zdroji,

[23] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR)…*, s. 232-234 (čl. 26)
[24] čl. 26 bod 8 nařízení
[25] zákon č. 256/2013 Sb., katastrální zákon, § 54 odst. 2

prostorami a infrastrukturou tak, aby bylo zajištěno jeho účinné fungování. Nakonec jde o personální nezávislost, kdy pracovníci mohou být řízeni pouze členy dozorového úřadu, tzn. že jednotlivé pracovníky úřadu vybere sám dozorový úřad a tito budou podléhat pouze vedení členů příslušného dozorového úřadu.[26]

V České republice je tímto nezávislým dozorovým úřadem Úřad pro ochranu osobních údajů. Současný zákon č. 110/2019 Sb., o zpracování osobních údajů upravuje tento dozorový úřad v § 50 a následujícím, kdy jej charakterizuje jako ústřední správní úřad pro oblast ochrany osobních údajů se sídlem v Praze.

Na úrovni EU byl zřízen Evropský sbor pro ochranu osobních údajů (European Data Protection Board, dále jako „EDPB“).[27] EDPB dle č. 70 GDPR zajišťuje jednotné uplatňování Obecného nařízení na poli EU, vydává nejrůznější pokyny pro dodržování nařízení a poskytuje také Komisi stanoviska. Cílem Komise je do budoucna prohloubit spolupráci mezi dozorovými úřady a EDPB. Další vizí je podpora zejména menších a středních podnikatelů v oblasti ochrany osobních údajů.[28]

[26] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR)…*, s. 361-3-362 (čl. 52)
[27] čl. 68 GDPR
[28] TZANOU, Maria. *Personal Data Protection and Legal Developments in the European Union*. UK: Keele University, 2020, s. 260

2 Pořizování záznamu bezpečnostní kamerou

2.1 Zásady zpracování osobních údajů

Dříve než se budu věnovat samotné otázce týkající se pořizování záznamu, je třeba připomenout bod 4 odůvodnění GDPR, kde je uvedeno, že zpracování osobních údajů by mělo sloužit lidem. Dále nařízení v tomto bodě hovoří o zásadě proporcionality. Zpracování osobních údajů totiž není absolutním právem a musí se proto posuzovat v souvislosti se svou funkcí ve společnosti. Aby právo na ochranu osobních údajů bylo skutečně v souladu se zásadou proporcionality, musí být toto právo zároveň v rovnováze i spolu s dalšími základními právy jedince.

Vedle zásady proporcionality je však třeba dbát i na další zásady zpracování osobních údajů, které Obecné nařízení v čl. 5 zakotvuje. Obecné nařízení předpokládá uplatnění zásad v něm uvedených na všechny informace, které se týkají fyzické osoby identifikované či identifikovatelné.[29] Kdo je osobou identifikovanou a kdo osobou identifikovatelnou je již vymezeno v první kapitole této diplomové práce. Pro pořizování záznamu a pro používání bezpečnostních kamer obecně je třeba zdůraznit, že takto může být činěno pouze za účelem dosažení legitimního cíle. Osobní údaje lze shromažďovat pouze pro určité, výslovně vyjádřené a legitimní účely a zároveň nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely.[30]

Za určitých okolností lze osobní údaje zpracovávat i pro jiné účely, než pro které byly původně shromažďovány. To by však mělo být povoleno pouze tehdy, když takovéto zpracování osobních údajů bude slučitelné s účely, pro které byly osobní údaje původně shromažďovány.[31] Z uvedeného vyplývá povinnost správce, stanovit účel, pro které bude osobní údaje zpracovávat. Kamerový systém je technický prostředek, kterým jsou osobní údaje zpracovávány. Jedná se tedy o způsob zpracování osobních údajů. Každý, kdo se rozhodne provozovat kamerový systém si musí stanovit, za jakým účelem tak bude činit. Legitimním účelem může být například ochrana majetku.[32]

[29] Bod 26 odůvodnění GDPR
[30] čl. 5 odst. b) GDPR
[31] bod 50 odůvodnění GDPR
[32] BARTÍK, Václav, JANEČKOVÁ Eva. *Zákon o ochraně osobních údajů s komentářem*. Olomouc: Anag, 2010. s. 71

2.2 Legitimní účel a problematika (ne)ohlášení bezpečnostní kamery

Při provozování kamerového sytému bude zákonným důvodem pro zpracování osobních údajů nejčastěji právní povinnost správce nebo bude provoz kamery nezbytný pro účely oprávněných zájmů správce či třetí osoby nebo bude zákonným důvodem souhlas dotčeného subjektu. V druhém případě bude oprávněným zájmem typicky ochrana majetku správce či třetí osoby. Musí však být naplněn předpoklad nezbytnosti zpracování ve vztahu k účelu, tedy např. k ochraně majetku. Dále je třeba, aby objektivně převážil zájem správce na monitorování určitého prostoru nad právem na ochranu soukromí člověka. K prvnímu případu, kdy správci sám zákon ukládá povinnost provozovat kamerový systém, můžeme uvést např. zákon č. 186/2016 Sb., o hazardních hrách.[33] Otázce souhlasu se budu ještě podrobněji věnovat v následujících částech této práce.

Otázkou dosažení legitimního cíle při provozování bezpečnostních kamer se poměrně často zabýval Nejvyšší správní soud. V této souvislosti lze uvést například rozsudek Nejvyššího správního soudu ze dne 3. května 2017, sp. zn. 7 As 36/2017. V citovaném rozhodnutí soud řešil případ, kdy bezpečnostní kamera umístěna na herně odhalila dopravní přestupek stěžovatele. V době spáchání přestupku však bezpečnostní kamera nebyla ohlášena Úřadu pro ochranu osobních údajů. Kamera byla následně ohlášena až v době, kdy správní orgán projednával spáchaný přestupek.

Správní orgán s ohledem na judikaturu Nejvyššího správního soudu a Ústavního soudu shledal, že přestože bezpečnostní kamera v době spáchání přestupku nebyla ohlášena Úřadu, jde o důkaz použitelný v přestupkovém řízení, neboť se jedná pouze o administrativní chybu a nedošlo k závažnému zásahu do soukromého a osobního života stěžovatele. [34]

Krajský soud provedl test proporcionality a dospěl k závěru, že není vyloučen zásah do žalobcovy soukromé sféry, neboť byla zachycena jeho tvář i postava. Nicméně kamerový systém byl zaveden za účelem zajištění vyšší bezpečnosti pro hosty i zaměstnance herny. Neoznámení kamerového systému Úřadu je pouhou formální chybou administrativního charakteru a nejde o porušení právních předpisů takové intenzity, kdy by kamerový záznam jako důkaz nemohl být použit. Navíc byl záznam určen jen pro omezený okruh osob.[35]

Ani Nejvyšší správní soud nezaujal jiné stanovisko. K otázce legitimního účelu uvedl, že tento má především zabránit tomu, aby záznamy pořízené z kamer umístěných z důvodu blížícího se špehování či voyerismu, byly označeny za přípustné. V tomto posuzovaném

[33] ŽŮREK Jiří. *Praktický průvodce GDPR*..., s. 216 – 217
[34] rozsudek Nejvyššího správního soudu ze dne 3. května 2017, sp. zn. 7 As 36/2017
[35] Tamtéž

případě naplnění legitimního cíle shledal, a to i přesto, že kamerový systém nebyl řádně a včas ohlášen Úřadu.[36]

S názorem soudů vyslovených v tomto případě nelze jinak než souhlasit. Opačný náhled na věc by byl ryze formalistickým nahlížením na splnění povinnosti k zavedení a provozu kamerového systému. V prvé řadě je potřeba zohlednit legitimní cíl, pro který byla kamera zavedena. V tomto případě šlo o zajištění bezpečnosti osob nacházejících se v příslušných prostorách. Tudíž podmínka legitimního účelu byla naplněna. Navíc k záznamu měl přístup pouze omezený počet osob, provozovatel dbal i na zabezpečení údajů kamerově získaných. V uvedeném případě byly naplněny všechny ostatní podmínky pro provoz kamery. Vyloučit kamerový záznam jako důkaz kvůli včasnému neohlášení by bylo v tomto případě nesmyslné s ohledem na konkrétní okolnosti tohoto případu.

2.3 Použití záznamu pro účely dokazování

Ve shora citovaném rozsudku je odkaz na jiné důležité rozhodnutí NSS, které se otázce přípustnosti kamerového záznamu jako použitelného důkazu také věnovalo a které nepochybně stojí za zmínku. Skutkový stav byl obdobný, rovněž šlo o dopravní přestupek, který zaznamenala bezpečnostní kamera umístěna na sportovní hale. Ani v tomto případě nedošlo k ohlášení kamery Úřadu. I zde se NSS přiklonil k tomu, že neohlášení bezpečnostní kamery samo o sobě nezpůsobuje nezákonnost takového důkazu. NSS zde řešil i otázku, kdo obrazový záznam pořídil, zda to byla soukromá osoba nebo zda orgán veřejné moci. V případě, že obrazový záznam pochází z bezpečnostní kamery orgánu veřejné moci, musí být takový postup výslovně předpokládán zákonem a musí být splněny všechny podmínky zákonem vyžadované. Jestliže obrazový záznam pochází z bezpečnostní kamery soukromé osoby, nejde takový záznam při nesplnění všech s tím spojených zákonných omezení pro potřeby dokazování a priori vyloučit.[37]

Protože se v praxi poměrně často stávalo, že bezpečnostní kamery nebyly Úřadu ohlášeny, tato situace následně vedla k tomu, že v případných správních či soudních sporech byla namítána nezákonnost takového obrazového záznamu. Nejvyšší správní soud v rámci své rozhodovací praxe tuto otázku řešil hned několikrát a právní názor soudu je v tomto ohledu neměnný. Právě v již zmíněném rozhodnutí Nejvyššího správní soudu ze dne 18. listopadu 2011, sp. zn. 2 As 45/2010 soud uvedl, že pokud s ohledem na konkrétní situaci obrazový

[36] rozsudek Nejvyššího správního soudu ze dne 3. května 2017, sp. zn. 7 As 36/2017
[37] rozsudek Nejvyššího správního soudu ze dne 18. 11. 2011 , sp. zn. 2 As 45/2010

záznam dotčené fyzické osoby nemohl zasáhnout do jejího práva na soukromí nebo práva na ochranu před neoprávněným pořizováním a používáním obrazových záznamů, lze takový záznam užít ve správním či soudním řízení. Nezáleží přitom, zda dotčená fyzická osoba vyjádřila s takovým postupem souhlas či nikoli. V případě, že je kamerový systém provozován bez ohlášení Úřadu a jím pořízený záznam má být ve správním či soudním řízení použit jako důkaz, je potřeba posoudit, zda zpracování osobních údajů probíhalo v rozporu či v souladu se zákonem.

2.4 Provozování kamerového systému jako zpracování osobních údajů

2.4.1 Vymezení pojmu soukromí

Dříve než se budu věnovat samotné otázce zpracovávání osobních údajů, je potřeba uvést, že pořizováním kamerových záznamů může být zasahováno do soukromí jiných osob. Právo na respekt k soukromému životu má zjistit možnost rozvoje a realizace individuální autonomní osobnosti. Soukromý život můžeme rozdělit do dvou oblastí, a to aktivní a pasivní oblast. Do aktivní oblasti patří právo rozhodovat o sobě samém, o uspořádání svého vlastního života. Pasivní oblast soukromého života zahrnuje především lidskou důstojnost, osobní čest, dobré jméno, potřeba sociálního kontaktu a začlenění. Právo na soukromý život tak zahrnuje nejen vnitřní, ale i vnější složku vztahující se k obchodním, pracovním či sociálním aktivitám. Lze tak vidět, že pojem soukromý život je velmi rozsáhlý, mnohovrstevnatý pojem, který nelze jednoduše charakterizovat. Můžeme jej však alespoň rozčlenit do čtyř oblastí, a sice 1) osobní soukromá sféra, 2) rodinný život a právo na uzavření manželství a založení rodiny, 3) soukromí v prostorové dimenzi (tedy obydlí) a 4) důvěrnost komunikace.[38]

V osobní soukromé sféře se právo na soukromý život projevuje jako negativní právo, tedy svoboda, to znamená právo, které brání veřejné moci zasahovat do osobní soukromé sféry. Dále se v této sféře právo na soukromý život projevuje i jako pozitivní závazek státu, zabránit třetím, soukromým osobám zasahovat do osobní sféry.[39] Pokud se podíváme na soukromí v prostorové dimenzi, tj. obydlí, zde musí zákonodárce přijmout takovou právní úpravu, která je způsobilá zajistit ochranu před zásahy třetích, soukromých osob. Může se jednat o zásahy spočívající v pořizování fotografií nebo zvukových záznamů v uzavřeném soukromém prostoru. V této sféře, tj, obydlí je chráněno soukromí jednotlivce nejen v prostorách nemovitostí, ale i movitých věcí. Není důležité ani to, zda člověk daný prostor užívá trvale nebo přechodně. Dokonce ani

[38] WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod: Komentář*. 3. vydání. Praha: Wolters Kluwer, 2012. 931 s. (čl. 10 Listiny)
[39] Tamtéž

vlastnictví nemovitosti nehraje roli. Prostorová ochrana soukromí je vykládána široce. Chráněny jsou i prostory související s bydlením, tedy např. garáže, sklepy, terasy, půdy, nezastavěné plochy jako dvory či zahrady.[40] Ochrana soukromí v prostorové dimenzi je důležitá zejména v případě kamerového systému bytového domu. Existují totiž jistá omezení, kdy kamera nemůže snímat kdejaké prostory v bytovém domě. Stejně tak ani v případě kamery rodinného domu. Ani v tomto případě není přípustné snímat kdejaké prostory. Tato problematika však bude řešena v další části této práce.

Obecně při pořizování obrazových záznamů a dalším zpracování takových záznamů lze získat množství informací, které budou mít nezanedbatelný dopad do soukromí takto dotčených osob, zejm. se může jednat o sociální vazby těchto osob. Soukromí jednotlivce zahrnuje i jeho právo navazovat a rozvíjet sociální vazby, a to nejen s bližními, ale spadají zde i profesionální nebo obchodní aktivity. [41] Na toto je potřeba pamatovat zejména v případech, kdy bude bezpečnostní kamera umístěna tak, že bude zabírat i část veřejné ulice nebo společné prostory v domě. Tím totiž umožní zjistit, například kdo navštěvuje lékařskou ordinaci nebo advokátní kancelář.[42]

Na základě výše uvedeného lze shrnout, že pojem soukromí je velmi obsáhlý pojem. Jedná se o základní právo, které je garantováno a chráněno čl. 8 Úmluvy, dále Listinou v čl. 7 odst. 1, čl. 10, čl. 12 a čl. 13. Při provozování kamerového systému bude v naprosté drtivé většině případu soukromí jednotlivce dotčeno. Bude tak potřeba striktně trvat na dodržení podmínek pro instalaci a provoz kamer, neboť z kamerového záznamu může být následně zjištěn nespočet informací vypovídající o soukromém životě dotčené osoby.

2.4.2 Osobní údaje získané z kamerového záznamu

Na otázku, zda při pořizování kamerového systému dochází ke zpracování osobních údajů, nešlo s jistotou vždy kladně odpovědět. V minulosti se touto otázkou NSS několikrát zabýval.

Judikatura je i v tomto směru konstantní. Nejvyšší správní soud při posuzování této otázky vycházel mimo jiné i ze Stanoviska Úřadu č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů. V tomto Stanovisku Úřad uvádí, že obrazové či zvukové údaje, které se uchovávají v záznamovém zařízení jsou osobními údaji, pokud na základě takových záznamů můžeme přímo nebo nepřímo identifikovat konkrétní fyzickou

[40] WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod…,* (čl. 12)
[41] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: Komentář*. Praha: Wolters Kluwer, 2014. 504 s. (čl. 4)
[42] Tamtéž

osobu. Dále uvádí, že identifikovatelná je fyzická osoba tehdy, když jsou ze záznamu patrné její charakteristické rozpoznávací znaky (především obličej) a spolu s dalšími disponibilními údaji, lze tuto osobu plně identifikovat. Osobní údaj tedy tvoří identifikátory umožňující příslušnou osobu spojit s určitým jednáním.

Od vydání tohoto Stanoviska sice uplynulo několik let a právní úprava mezitím doznala jistých změn, avšak s ohledem na současné znění GDPR se situace nijak podstatně nezměnila.[43]

Lze uzavřít, že provozováním kamerových systémů dochází ke zpracování osobních údajů, pokud se však nejedná o pouhé kamerové sledování, ale naopak je prováděn záznam. Informace o subjektech jsou tedy uchovávány. Navíc účelem je, pořízené, příp. vybrané informace následně užít pro identifikaci fyzických osob v souvislosti s určitým jednáním.[44]

Tento závěr byl ostatně potvrzen i NSS, který uvedl, že pokud jsou obrazové či zvukové údaje uchovávány v kamerovém zařízení se záznamem a na základě tohoto záznamu lze identifikovat konkrétní osobu, jedná se o zpracování osobních údajů. Navíc účelem dohledu prostřednictvím kamery je následná identifikace osob, které kamera zachytila, proto je potřeba provoz kamerového systému považovat za zpracování osobních údajů. I v případě, že kamerový záznam zachytí jistou osobu, avšak tuto osobu nebude možno identifikovat, neznamená to automaticky vyloučení aplikace zákona o ochraně osobních údajů. Ztotožnit osoby zachycené na obrazovém záznamu nemusí být možné například proto, že se daná osoba zamaskuje nebo z důvodu negativních pozorovacích podmínek (například pokud venku bude mlha nebo kamera bude snímat v noci). Pokud by k takovéto situaci došlo, neznamená to, že nejde o zpracování osobních údajů a že se neuplatní zákon o ochraně osobních údajů. Opačná situace by byla, kdyby kamera nebyla schopna zachytit identifikovatelným způsobem žádnou osobu, pak by bylo i nesmyslné vůbec pořízení si takové kamery. [45]

2.4.3 Požadavek subsidiarity

V souvislosti se zamýšlenou instalací kamerového systému je potřeba upozornit na to, že k tomuto kroku lze přistoupit až tehdy, kdy legitimního cíle nelze dosáhnout prostředky, které představují menší zásah do soukromí.[46]

Při provozování kamerového systému tak musíme dbát na zásadu subsidiarity. Na tuto zásadu upozorňoval ve svých rozhodnutích i NSS. Jelikož jde o zásah do osobní integrity,

[43] čl. 4 nařízení GDPR
[44] BARTÍK, Václav, JANEČKOVÁ Eva. *Zpracovávání osobních údajů obcemi. Vybrané problémy*. Praha: Wolters Kluwer, 2013. s 106
[45] rozsudek NSS ze dne 25. února 2015, sp. zn. 1 As 113/2012, bod 37
[46] ŽŮREK Jiří. *Praktický průvodce GDPR...*, s. 217

k instalaci kamerových záznamů je proto možné přistoupit až v případě, že všechny prostředky, které nejsou tak invazivní, již selhaly anebo by takové prostředky nebyly schopny naplnit účel, který chce pořizovatel sledovat. Kamerový systém totiž zasahuje do základních lidských práv, konkrétně do práva na soukromí a do práva na soukromý a rodinný život garantovaných čl. 10 Listiny a čl. 8 Úmluvy. Rovněž zasahuje i do lidské důstojnosti, z níž tato práva vyplývají. Ve vztahu k legitimnímu účelu provozování bezpečnostní kamery, NSS je seskupil do několika hlavních kategorií: „*1) ochranu jednotlivců, 2) ochranu majetku, 3) veřejný zájem, 4) odhalování, prevence a stíhání trestné činnosti, 5) získávání důkazů a 6) jiné legitimní zájmy*."[47]

2.5 Test proporcionality

2.5.1 Obecně k poměřování v kolizi stojících základních práv

Soukromí jednotlivce patří mezi základní práva garantována Listinou. Toto právo ale může být omezeno. Musí se však jednat o omezení restriktivní, kdy pojistkou pro zajištění restriktivního omezení tohoto základního práva je uplatnění principu proporcionality. Tento princip zajišťuje existenci materiálního obsahu práva na soukromí. Je nezbytné, aby v každém konkrétním případě docházelo jen k nutnému a spravedlivému omezení práva na soukromí, aby mohl být naplněn účel omezení základního práva. Omezení práva na soukromí tak musí být vhodné, tedy věcně souviset s účelem a musí být potřebné pro dosažení daného cíle, kdy neexistuje jiný mírnější prostředek k dosažení stanoveného cíle. Zároveň omezení práva na soukromí musí být proporcionální k významu sledovaného cíle. Jinými slovy, nesmí dotčeného jedince zatěžovat přehnaně či neúnosně. Pokud budou tyto předpoklady naplněny, jednotlivec musí újmu na právu na svém soukromí přijmout. Dá se říct, že čím více se zásah dotýká intimní sféry jednotlivce, tím jsou na proporcionalitu takového zásahu kladeny vyšší nároky.[48]

V testu proporcionality jde o posuzování možnosti omezení základního práva či svobody ve prospěch jiného základního práva či svobody. Vzájemné poměřování v kolizi stojících základních práv či svobod spočívá ve třech kritériích. Zaprvé jde o kritérium *vhodnosti,* tzn. zda institut omezující dané základní právo umožňuje dosáhnout sledovaného cíle. Zadruhé jde o kritérium *potřebnosti*, tzn. zda zvolený prostředek omezující základní právo či svobodu umožňuje dosáhnout stejného cíle, jako jiný prostředek, který se natolik nedotýká základních práv či svobod. Poslední třetí kritérium spočívá v *porovnání* závažnosti obou v kolizi se nacházejících základních práv či svobod.[49]

[47] rozsudek Nejvyššího správního soudu ze dne 23. 8. 2018, sp. zn. 5 As 158/2012
[48] WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod…* (čl. 10 Listiny)
[49] nález Ústavního soudu ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94

2.5.2 Zpracování osobních údajů výlučně pro osobní či domácí potřebu

K Nejvyššímu správnímu soudu se dostal případ, kdy stěžovatel v roce 2007 umístil na rodinný dům bezpečnostní kameru. Důvodem byly předcházející opakované útoky nejen na osobu stěžovatele, ale i na členy jeho rodiny a dále útoky směřující na stěžovatelův majetek. Dle Úřadu se stěžovatel dopustil přestupku, neboť neoprávněně shromažďoval osobní údaje jiných osob, tyto osoby o této skutečnosti neinformoval a dále nesplnil oznamovací povinnosti o zpracování osobních údajů vůči Úřadu. Stěžovatel totiž umístil kameru tak, že zabírala nejen jeho pozemek, ale i část veřejné ulice.[50]

Nejvyšší správní soud řízení přerušil a položil Soudnímu dvoru Evropské unie předběžnou otázku, zda „*lze provozování kamerového systému umístěného na rodinném domě za účelem ochrany majetku, zdraví a života majitelů domu podřadit pod zpracování osobních údajů „prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností" ve smyslu čl. 3 odst. 2 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, s. 31; Zvl. vyd. 13/15, s. 355), třebaže takovýto systém zabírá též veřejné prostranství*?" [51]

Soudní dvůr Evropské unie na tuto předběžnou otázku odpověděl tak, že pokud je provozován kamerový systém, při kterém je obrazový záznam zachycující osoby ukládán formou nekonečné smyčky na pevný disk a který umístila fyzická osoba na svůj rodinný dům za účelem ochrany života, zdraví a majetku majitelů domu a takovýto záznam zabírá i veřejné prostranství, pak tento provoz kamerového systému nepředstavuje zpracování osobních údajů výlučně pro osobní či domácí potřebu.[52]

Usnesením ze dne 22. prosince 2014, sp. zn. 1 As 113/2012 pokračoval NSS v řízení. U principu proporcionality zhodnotil soud všechna kritéria stanovena Ústavním soudem.

Kritérium vhodnosti bylo splněno, když podstatou kamerového systému bylo vyhotovit záznam, který následně mohl vést k identifikace pachatele a jeho eventuálnímu odsouzení.[53]

Kritérium potřebnosti bylo rovněž naplněno. S ohledem na předcházející opakované útoky byl kamerový systém potřebný pro zajištění ochrany majetku, zdraví a života stěžovatele a jeho rodiny. Stěžovatel zavedl kamerový systém až poté, co jiné prostředky ochrany, jako například zvýšení ochranné zdi v zadní části domu nebo bezpečnostní skla s atrapou kamery, selhaly a

[50] rozsudek Nejvyššího správního soudu ze dne 25. února 2015, sp. zn. 1 As 112/2012
[51] usnesení Nejvyššího správní soudu ze dne 20. března 2013, sp. zn. 1 As 113/2012
[52] Rozsudek ze dne 11. prosince 2014, *Ryneš v. Úřad pro ochranu osobních údajů*, C-212/13, bod 35
[53] rozsudek Nejvyššího správního soudu ze dne 25. února 2015, sp. zn. 1 As 112/2012

útoky na stěžovatele pokračovaly i nadále. Při jednom útoku došlo k prostřelení okna v době, kdy byli všichni rodinní příslušníci doma. Jelikož se policii nepodařilo pachatele dopadnout, byl stěžovatel následně nucen k pořízení kamerového systému. Kamera stěžovatele zabírala nejen jeho pozemek, ale i ulici a vchod do protějšího domu. Toto však bylo logicky zdůvodněno tím, že v opačném případě by se kamerový systém mihl účinkem, jelikož by pachatele nikdy nezachytil. [54]

I třetí kritérium, tj. porovnání závažnosti v kolizi stojících základních práv bylo naplněno. Stěžovatel sice snímal část veřejného prostranství a dokonce i vstup do protějšího domu, nicméně na tomto místě soud uvedl, že je potřeba rozlišovat vstup do bytu nebo přímo do obydlí na jedné straně a na straně druhé vstup do bytového domu z veřejné ulice, který je však přístupný širší veřejnosti a vede do společných prostor, kde se nachází schránky, schodiště apod. Snímání vstupu do obydlí se bude zcela jistě posuzovat přísněji než snímání vstupu do společných prostor bytového domu, jelikož společné prostory domu neposkytují takovou míru soukromí jako samotný byt. V posuzovaném případě byl snímán vstup do domu, kde byly nebytové prostory jako jsou kavárna a obchody. Vstup do obytného domu byl až ze dvora, tudíž nebyl nijak dotčen osobní život obyvatelů konkrétního bytu. [55]

Nyní posuzovaný případ byl extrémní, neboť šlo o reakci na opakované a závažné útoky vůči stěžovateli i jeho rodině, tudíž hrozba útoků byla velice reálná, a dokonce vedla k usvědčení pachatele této trestné činnosti. Jelikož však Úřad pro ochranu osobních údajů posuzoval podmínky instalace a provozu kamerových záznamů velmi přísně, Nejvyšší správní soud v tomto rozsudku zároveň zdůraznil, že je potřeba vždy brát v úvahu, zda provoz kamerového systému má zabránit útokům, které na daném místě hrozí nebo dokonce jde o reakci na již opakované útoky na ústavně zaručené hodnoty, anebo je naopak kamera instalována z pouhé obavy před protiprávní činnosti, která je pouze hypotetická a s ohledem na všechny okolnosti spíše nepravděpodobná.[56]

2.5.3 Případ, který neprošel testem proporcionality

Dalším zajímavým případem, který NSS řešil, bylo umístění kamery v přední části autobusu. Stěžovatelka měla v úmyslu umístit kameru tak, že obrazový záznam by zabíral řidiče a stevarda. Úřad takovéto zpracování osobních údajů nepovolil. NSS provedl test proporcionality, kdy kritérium vhodnosti bylo naplněno, neboť kamerové systémy mají

[54] Tamtéž
[55] Tamtéž
[56] rozsudek Nejvyššího správního soudu ze dne 25. února 2015, sp. zn. 1 As 112/2012

významný vliv při následném uplatnění práv poškozeným, mohou zabránit opakování protiprávního jednání v budoucnu a představují i odstrašující prvek ve vztahu právě k protiprávnímu jednání. Ve druhém kroku NSS zkoumal kritérium potřebnosti. Došel ale k závěru, že v posuzovaném případě stěžovatelka neprokázala reálné ohrožení právem chráněných hodnot. Rovněž nebylo prokázáno, že by se stěžovatelka prvně pokusila použít jiné, méně invazivní prostředky a nebylo zřejmé ani to, že by tyto jiné prostředky nevedly k dosažení zamýšleného cíle. Cílem totiž měla být ochrana majetku stěžovatelky, jejich zaměstnanců a cestujících. [57]

NSS dále porovnával sledování cestujících prostřednictvím obrazového záznamu a sledování případnými kontrolory. Byť by nebyl prostřednictvím kamerového záznamu zaznamenáván zvuk, pořád jde o výraznější zásah do soukromí cestujících. Pokud totiž dochází ke sledování určité osoby bez jakéhokoliv záznamu, jsou osobní údaje uchovávány jen v omezeném rozsahu v paměti cestujících. Jestliže se ale záznam uchovává například na pevném disku, je možné následně tento záznam znovu přehrát a zaměřit se i na různé detaily.[58]

Uvedený případ byl odlišný oproti tomu předcházejícímu hned v několika aspektech. V nyní posuzovaném případě stěžovatelka svůj záměr zavést kamerový systém prve konzultovala s Úřadem, tento však instalaci kamery nepovolil. Další odlišnost spočívá v tom, že zde hrozící nebezpečí bylo pouze hypotetické, nebylo prokázáno, že by v minulosti došlo k nějakým zásahům do stěžovatelčiných práv. Stejně tak nebyl dodržen ani požadavek subsidiarity ve vztahu k zavedení kamerového systému. Z těchto důvodu tedy zamýšlené zpracovávání osobních údajů prostřednictvím kamerového systému neprošlo testem proporcionality.

2.6 Zákonnost zpracování osobních údajů

Jelikož již byla vyjasněna otázka zpracování osobních údajů, je potřeba, aby bylo toto zpracování zákonné. O zákonné zpracování osobních údajů jde tehdy, pokud je splněna alespoň jedna z podmínek uvedených v čl. 6 Nařízení: *a) subjekt udělil souhlas se zpracování osobních údajů*, nebo je zpracování osobních údajů nezbytné pro *b) plnění smlouvy nebo před uzavřením smlouvy a subjekt údajů je nebo bude stranou smlouvy, c) splnění právní povinnosti správce, d) ochranu životně důležitých zájmů, e) splnění úkolu ve veřejném zájmu či při výkonu veřejné moci* nebo *f) účely oprávněných zájmů správce či třetí strany.*

[57] rozsudek Nejvyššího správního soudu ze dne 20. prosince 2017, sp. zn. 10 As 245/2016
[58] Tamtéž

Otázka souhlasu se zpracováním osobních údajů může být v praxi v souvislosti s kamerovým záznamem problematická, této otázce se budu více věnovat v další části této práce.

V souvislosti s provozováním kamerového systému bude nejčastějším právním důvodem, o který se bude provozovatel opírat, oprávněný zájem. Jedná se o poměrně flexibilní právní titul. Jestliže lze daný zájem označit za oprávněný a pro dosažení tohoto zájmu bude nezbytné zpracovávat osobní údaje, je možné tak učinit. V případě, že nad oprávněným zájmem v konkrétním případě převáží zájmy či základní práva a svobody subjektu údajů, jejichž osobní údaje mají být zpracovávány, pak v takovém případě tyto osobní údaje zpracovávat nelze. Tudíž ještě, než správce přistoupí ke zpracovávání osobních údajů na základě tohoto právního titulu, musí nejdříve svůj oprávněný zájem posoudit. Musí zhodnotit oprávněnost stanoveného zájmu, dále to, zda je zamýšlené zpracování opravdu nezbytné pro dosažení stanoveného cíle a konečně, zda nad jeho zájmem nepřevažují zájmy nebo práva a svobody subjektu údajů. Pokud bude odpovědět na všechny tři body posouzení kladná, pak lze přistoupit ke zpracování osobních údajů.[59]

2.7 Ochrana osobnosti člověka

2.7.1 Soukromí člověka

Přestože bude dodržena podmínka zákonnosti zpracování osobních údajů, je potřeba zároveň dbát na ochranu osobnosti člověka poskytovanou občanským zákoníkem. Ustanovení § 84 a násl. občanského zákoníku upravuje podmínky, za kterých lze zachytit podobu člověka. V § 86 občanského zákoníku je zakotven zákaz zásahu do soukromí jiného člověka, aniž by k tomuto byl zákonný důvod. Zejména je zakázáno narušit soukromé prostory člověka bez jeho souhlasu, dále nelze sledovat soukromý život člověka a pořizovat o tom zvukový či obrazový záznam, využívat takové záznamy nebo je šířit.

Zákon pracuje s pojmem soukromí, vyvstává tak otázka, co všechno zahrnuje pojem soukromí. ESLP se tímto pojmem zabýval zejména při interpretaci čl. 8 Úmluvy. Výklad pojmu soukromí je poměrně extenzivní, neboť do tohoto práva jsou řazena různá dílčí osobnostní práva, jako jsou například právo na čest a důstojnost, právo na tělesnou integritu, právo na ochranu soukromých prostor, právo informačního sebeurčení, právo na jméno atd. ESLP vychází z toho, že základním principem při vymezení pojmu soukromý život, je jistá soukromá zóna, do níž není nikdo oprávněn vstupovat ani jinak zasahovat.[60]

[59] NULÍČEK, Michal a kol. *GDPR/Obecné nařízení o ochraně osobních údajů…* (čl. 6 GDPR)
[60] MELZER, Filip, TÉGL, Petr a kol. *Občanský zákoník – velký komentář. Svazek I. § 1 – 117*. Praha: Leges, 2013, s. 551 -552 (§ 86)

3 Prostory kamerově sledované a informační povinnost

3.1 Rozsah záběru kamery

Při instalaci a následném provozování bezpečnostní kamery je důležité, kde je kamera umístěna a jaké prostory snímá. Prvně je třeba si připomenout, že pokud je kamera nainstalovaná tak, že zabírá i jiné prostranství než jen výlučně pořizovatelův pozemek, nejde o zpracování osobních údajů výlučně pro osobní či rodinné potřeby a uplatní se tak evropská právní úprava, tedy Obecné nařízení.

Legalita snímání i jiného než vlastního pozemku, je dána účelem, za kterým je kamerový systém pořizován. V případě ochrany majetku, zdraví a života pořizovatele a jeho rodinných příslušníků pak může záznam z kamery sloužit k identifikaci pachatele. K útokům na tyto chráněné hodnoty však může dojít i zpovzdálí, a proto je logické, že kamerový systém zaznamenává i část cizího pozemku, a to právě za účelem naplnění legitimního cíle, pro který pořizovatel přistoupil ke kamerovému snímání.

Úřad pro ochranu osobních údajů často odpovídal na dotazy, zda lze snímat i jiný pozemek než svůj vlastní. Dle Úřadu je přípustné, aby kamera snímala vedle vlastní nemovitosti přiměřeně také její hranici, jako jsou okrajové části přilehlých zahrad, polí či veřejných komunikací.[61] Právě z těchto míst totiž často pochází útok na chráněné zájmy. Při instalaci kamery tak musí být dodržena zásada minimalizace zpracování osobních údajů[62], kdy kamera nesmí zabírat veřejné prostranství více, než je nezbytné pro identifikaci útočníka proti plášti budovy nebo oplocení soukromého pozemku. Výše jsem uvedla, že pokud jsou snímány i jiné prostory než výlučně provozovatele kamerového systému, uplatní se Obecné nařízení. Toto Úřad upřesňuje, když říká, že pod režim Obecného nařízení bude spadat až snímání veřejného prostranství ve větším rozsahu. V takovém případě pak bude toto snímání přípustné pouze výjimečně, například pokud bude docházet k opakovaným útokům na chráněné zájmy právě z veřejného prostranství.[63]

Přípustnost kamerového snímání i části jiných prostorů než jen vlastních nemovitostí, je logické zejména z pohledu účelu zavedení kamer. Legitimním účelem totiž bude často ochrana majetku, života a zdraví osob. Útok na tyto chráněné statky však muže přijít i zpovzdálí. Pokud by kamera snímala výlučně vlastní nemovitost, mohlo by to znemožnit identifikaci pachatele.

[61] Úřad pro ochranu osobních údajů. *Co dělat, když soused používá kameru*? [online]. uoou.cz, 2. 5. 2018 [cit. 20. března 2020]. Dostupné na < https://www.uoou.cz/co-delat-kdyz-soused-pouziva-kameru/ds-5283/archiv=0&p1=2619>.

[62] čl. 5 odst. 1 písm. c) GDPR

[63] Úřad pro ochranu osobních údajů. *K provozování kamerových systémů* [online]. uoou.cz, 2. 5. 2018 [cit. 20. března 2020]. Dostupné na < https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099>.

Kamera by pak neposloužila účelu, pro který byla zavedena. Jak velkou část „cizích“ prostor lze snímat není nikde uvedeno. Zcela jistě však nebude přípustné sledovat vedle vlastní nemovitosti i celý sousedův pozemek nebo ulici, kde se příslušný dům nachází. Jako přípustné si naopak lze představit snímání okrajových částí jiných vedlejších pozemků v řádu několika pár metrů od společné hranice. Každý případ je však individuální a bude tak záležet na konkrétních okolnostech.

3.2 Zaznamenávání i jiných než vlastních nemovitostí

Situací, kdy kamera snímá i jiné nemovitosti než jen nemovitost pořizovatele, se zabýval NSS ve svém rozhodnutí ze dne 20. září 2017, sp. zn. 2 As 140/2017. V posuzovaném případě stěžovatel umístil bezpečnostní kameru na svůj rodinný dům, avšak kamera zabírala nejen stěžovatelův pozemek a nezbytné části veřejné komunikace, ale i sousední nemovitost ve vlastnictví třetích osob. Stěžovatel si od vlastníků sousední nemovitosti nevyžádal souhlas se zpracováním osobních údajů. Důvodem zavedení kamery byly údajné opakované útoky ze strany sousedů na jeho majetek. Stěžovateli se ale nepodařilo prokázat, že by k takovýmto útokům ze strany sousedů skutečně došlo, přestože se opakovaně obracel na Polici ČR. Ani poté, co zavedl kamerový systém, nebyly žádné útoky na jeho majetek zaznamenány. K otázce absence souhlasu, stěžovatel uvedl, že tento získal od Police ČR. NSS se ztotožnil se závěry Městského soudu v Praze, který k tomuto uvedl, že pokud byl dán souhlas ke sledování osob a věcí ve smyslu § 158d zákona č. 141/1961 Sb., trestního řádu, mohl směřovat pouze vůči orgánům činným v trestním řízení. Státní zastupitelství nedisponuje oprávněním dát takový souhlas soukromé osobě.

V uvedeném případě tedy nebyly splněny zákonné podmínky pro monitorování prostorů mimo stěžovatelův pozemek v takovém rozsahu, v jakém jej stěžovatel prováděl. Kamera stěžovatele zabírala hned několik nemovitostí včetně nemovitosti souseda. Navíc nebezpečí zásahu na chráněné statky nebylo ani v minulosti ani po zavedení kamery prokázáno. Také nesmíme odhlédnout od toho, že monitorováním rozsáhlé části sousedova pozemku došlo k výraznému zásahu do jeho soukromého života, a to, aniž by s tímto vyslovit souhlas. Závěr NSS je tak v tomto případě zcela správný.

3.3 Zásada transparentnosti

V rámci provozu bezpečnostních kamer dochází k realizaci jednoho ze základních práv a sice práva na informace. Ani obecné nařízení toto právo neopomíjí, když v čl. 5 odst. 1 písm. a)

zakotvuje zásadu transparentnosti, jakožto jednu ze stěžejních zásad pro zpracovávání osobních údajů obecně. Podstata spočívá v povinnosti správců poskytnout subjektům údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem potřebné informace, to vše za použití jasných a jednoduchých jazykových prostředků. Tyto informace lze poskytnout ústně, písemně, elektronicky či jiným způsobem. Rovněž mohou být tyto informace doplněny ikonami.[64]

Aby byl zajištěn požadavek stručnosti a transparentnosti, bude správce využívat různé vizualizace, členění textu, druhy písma apod. Zároveň musí dbát na to, aby čtenáře nezahltil příliš dlouhým textem. Pro naplnění požadavku srozumitelnosti musí správce poskytovat informace v takové formě, aby je pochopil průměrný adresát. Snadno přístupné informace, jako další požadavek, jsou pak takové informace, které adresát nemusí vyhledávat. Buď by jim měly být informace přímo předloženy nebo by mělo být zjevné, kde tyto informace naleznou. Je také potřeba dbát na to, aby zvolený způsob poskytování informací odpovídal konkrétním okolnostem, s ohledem na způsob běžné komunikace správce a subjektu údajů nebo způsobu shromažďování osobních údajů. Další požadavek, a sice požadavek užití jednoduchých jazykových prostředků, znamená podávání informací tím nejjednodušším způsobem. Správce by neměl používat dlouhá souvětí nebo právnický jazyk. Velmi důležité je, aby co nejjasněji byl vymezen účel a právní důvod zpracování osobních informací.[65]

3.4 Informace o zpracovávání osobních informací

Pro splnění informační povinnosti správce údajů je důležitý také časový okamžik, kdy bude subjekt údajů informován o tom, že dochází ke zpracovávání jeho osobních údajů. Na to pamatuje Obecné nařízení, když uvádí, že informační povinnost ohledně zpracovávání osobních údajů by měla proběhnout ve chvíli, kdy správce údajů informace shromažďuje. Pokud jsou však informace získávány z jiného zdroje než přímo od samotného správce údajů, informační povinnost má být splněna v přiměřené lhůtě.[66] Co je onou přiměřenou lhůtou nelze jednoznačně určit. Lhůta bude závislá na konkrétních okolnostech daného případu.

V případě kamerových systémů s ohledem na požadavky, jak mají být informace poskytnuty, bude pravděpodobně nejefektivnějším způsobem umístění informační cedule s ikonou kamery. Zároveň by tato informační cedule měla být umístěna při vstupu do monitorovaného prostoru, aby byl subjekt údajů předem informován o této skutečnosti a mohl

[64] čl. 12 odst. 1, odst. 7 GDPR
[65] NULÍČEK, Michal a kol. *GDPR/Obecné nařízení o ochraně osobních údajů…*, s. 192 - 193 (čl. 12 GDPR)
[66] bod 61 GDPR

se rozhodnout, zda vstoupí do takového prostoru či nikoli. Tomu odpovídá i úvaha soudu, který uvedl, že jestliže dotyčná osoba ví o kamerovém systému, a přesto vstoupí do takto střeženého místa, dává tím konkludentní souhlas se zpracováním osobních údajů.[67]

Už tedy jen z tohoto důvodu by měly být informační cedule dobře viditelné ještě před vstupem do objektu. Samotná informace o tom, že daný prostor je monitorován kamerami však stačit nebude. Subjekt údajů musí být dále informován o tom, kdo zpracovává osobní údaje a jakým způsobem tak činí. Správce bude muset poskytnou informace o jeho totožnosti a jeho kontaktních údajích (buďto samotného správce či jeho zástupce), dále o účelu zpracování osobních údajů a na základě jakého právního důvodu tak činí. Pokud budou zákonným důvodem zpracování osobních údajů oprávněné zájmy správce či třetí osoby, musí rovněž uvést o jaké konkrétní oprávněné zájmy jde. Další informační povinnost správce spočívá v informování o případných příjemcích osobních údajů. Z důvodu zajištění transparentního a spravedlivého zpracování může subjekt údajů vyžadovat informace například o době uložení osobních údajů či možnosti podat stížnost u dozorového úřadu.[68]

Dle mého názoru není třeba na informační ceduli uvádět všechny výše uvedené informace, pokud tam bude uvedeno, kde lze tyto informace získat. Cedule by však vždy měla obsahovat informaci o tom, že prostor je monitorován a alespoň osobu správce a jeho kontaktní údaj.

[67] viz rozsudek Nejvyššího správního soudu ze dne 22. srpna 2019, sp. zn. 2 As 284/2018, bod 23
[68] HRUŠKA, Vít. *Právní úprava kamerových systémů podle GDPR*. [online]. maceklegal.cz, [cit. 4. března 2020]. Dostupné na <https://www.maceklegal.cz/pravni-uprava-kamerovych-systemu-podle-gdpr.html>.

4 Souhlas se zpracováním osobních údajů

Jedním ze zákonných důvodů zpracování osobních údajů je souhlas subjektu údajů. Vedle souhlasu lze osobní údaje zpracovávat i tehdy, pokud je zpracování nezbytné pro účely uzavření smlouvy, splnění právní povinnosti správce, ochranu životně důležitých zájmů, splnění úkolu ve veřejném zájmu či při výkonu veřejné moci nebo pro účely oprávněných zájmů správce nebo třetí strany.[69] Obecně tak můžeme říct, že souhlas není jediným právním titulem pro zpracování osobních údajů, není tedy nezbytný pro každé zpracování osobních údajů. Ještě, než správce přistoupí ke zpracování osobních údajů, měl by si položit otázku, zda může osobní údaje zpracovávat i na základě jiného právního titulu, než je souhlas. Souhlas by však měl být vyžadován tehdy, když je zpracování osobních údajů pro fyzické osoby nějakým způsobem rizikové a jiný právní titul užít nejde.[70] Tak tomu může být zejména v případě zavedení kamerového systému v obytných domech, proto jsem se také rozhodla věnovat problematice souhlasu se zpracováním osobních údajů samostatnou kapitolu.

4.1 Náležitosti souhlasu

Podmínky vyjádření souhlasu se zpracováním osobních údajů jsou uvedeny v čl. 7 Obecného nařízení. Souhlas musí být předně svobodný, tzn. že záleží pouze na úvaze subjektu údajů, zda takový souhlas poskytne nebo ne. S tím pak souvisí i možnost subjektu údajů souhlas kdykoliv odvolat. Dále je potřeba, aby byl souhlas informovaný, tzn. že subjekt údajů musí vědět, za jakým účelem budou jeho osobní údaje zpracovávány, kdo je správcem, jaké údaje budou zpracovávány a že má možnost souhlas kdykoliv odvolat. Další podmínkou je, aby byl udělený souhlas jednoznačný, tedy že nevzniknou pochybnosti o tom, zda byl udělen nebo ne. Jednoznačným souhlasem bude prohlášení nebo jiné zjevné potvrzení o souhlasu se zpracováním osobních údajů. Na tomto místě je třeba zdůraznit, že jednoznačným souhlasem nikdy nemůže být nevyjádření nesouhlasu. Vedle písemné formy souhlasu není vyloučeno ani konkludentní udělení souhlasu. To, že souhlas musí být jednoznačný, ještě nutně neznamená, že musí být i výslovný (srov. čl. 9 odst. 2 písm. a) nebo čl. 22 odst. 2 písm. c) GDPR, kde hovoří o výslovném souhlasu).[71]

[69] čl. 6 GDPR
[70] NULÍČEK, Michal a kol. GDPR v otázkách a odpovědích. *Bulletin advokacie*, 2017, č. 9, s. 33.
[71] PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR)…*,s. 103 – 106 (čl. 7)

Dle judikatury je konkludentní souhlas s pořizováním záznamu ve vztahu k dotčené osobě udělen tehdy, pokud tato osoba ví o tom, že určitý prostor je monitorován kamerami (byť tento prostor není označen informační cedulí) a přesto do tohoto prostoru dobrovolně vstoupí.[72]

4.2 Otázka souhlasu v souvislosti s užitím záznamu v řízení

Pokud se podíváme obecně na dokazování ve správním řízení, tak § 51 odst. 1 správního řádu uvádí, že jako důkaz lze užít všechny důkazní prostředky vhodné ke zjištění stavu věci, pokud nejsou získány nebo provedeny v rozporu s právními předpisy. Kamerový záznam, který bychom chtěli užít v řízení, by se mohl dostat do rozporu s občanským zákoníkem, GDPR či zákonem o zpracování osobních údajů. Podle § 88 občanského zákoníku souhlasu dotčeného jedince není třeba, jestliže se záznam pořídí nebo použije k výkonu či ochraně jiných práv nebo právem chráněných zájmů jiných osob.[73]

Co se týče možného rozporu s Obecným nařízením, výše jsem uvedla, že souhlas není jediným zákonným titulem pro zpracování osobních údajů. Například pokud budou osobní údaje zpracovávány za účelem ochrany oprávněných zájmů správce či třetí strany, pak je naplněn zákonný titul pro zpracování osobních údajů. Vedle toho však musí být naplněny i další podmínky proto, abychom mohli říct, že kamerový záznam byl získán v souladu s právním předpisem. Zejména je třeba splnění informační povinnosti ohledně prováděného zpracování osobních údajů (tedy min. účel zpracování a kontaktní údaje správce), dále dostatečné zabezpečení získaných údajů a také pouze nezbytně nutná doba uchovávání záznamů. Jestliže budou splněny uvedené předpoklady, pak byl kamerový záznam pořízen v souladu s právními předpisy a takový důkaz je možné uplatnit v případném správním řízení.[74]

K otázce souhlasu s pořízením záznamu a s tím související otázkou použitelnosti takového záznamu v případném správním či soudním řízení, se vyjadřoval NSS. Rozsudek, který uvedu se vztahuje k právní úpravě účinné ještě před přijetím Obecného nařízení, nicméně mám za to, že právní názory v něm uvedené lze aplikovat i za současné právní úpravy. Jedná se o rozsudek ze dne 18. listopadu 2011, sp. zn. 2 As 45/2010. V uvedeném rozhodnutí soud uvedl, že pokud byl kamerový záznam zasahující do osobnostních práv dotčené osoby pořízený soukromou osobou bez souhlasu dotčené osoby a není ani v souladu se zákonnými výjimkami (§ 5 odst. 2 zákona o ochraně osobních údajů), nelze automaticky hovořit o nepoužitelnosti takového

[72] rozsudek Nejvyššího správního soudu ze dne 22. srpna 2019, sp. zn. 2 As 284/2018, bod 23
[73] BUREŠOVÁ, Radana. *Kamerový záznam jako důkaz poškození majetku* [online]. fulsoft.cz, 14. března 2018 [cit. 25. července 2020]. Dostupné na < https://www.fulsoft.cz/33/kamerovy-zaznam-jako-dukaz-poskozeni-majetku-uniqueidmRRWSbk196FNf8-jVUh4EphuCjGAxFFf2R58d4zq4ddrJfTGJxQrnQ/>.
[74] Tamtéž

záznamu pro potřeby dokazování ve správním řízení. V takových případech bude vždy nutné poměřit legitimitu cíle, kterého mělo být dosaženo a přiměřenost použití takového postupu. Vždy bude třeba zvážit, zda v konkrétním případě může nad ochranou osobnostních práv převážit zájem společnosti na objasnění a potrestání protiprávních jednání, a především i ochrana ústavně zaručených práv pořizovatele záznamu.

Na základě výše uvedeného tak lze uzavřít, že neposkytnutí souhlasu se zpracováním osobních údajů v případě kamerového snímání nemusí nezbytně nutně mít za následek nepoužitelnost tohoto záznamu ve správním či soudním řízení. Je třeba zohledňovat i jiné aspekty, které mohou hrát důležitou roli v otázce připuštění takového záznamu pro účely dokazování ve správním řízení.

4.3 Souhlas se zpracováním osobních údajů v obytných domech

4.3.1 Monitorované prostory

Specifičtější úpravu užívání kamerových systému mají obytné domy. K otázce instalace a provozu kamerového systému v obytném domě s bytovými jednotkami se vyjadřoval Úřad ve svém Stanovisku č. 1/2016: Umístění kamerových systémů v bytových domech.[75] Na tomto místě Úřad uvedl, že je potřeba přihlížet k povaze prostor, jež mají být monitorovány. Záleží na tom, zda jsou takové prostory obvykle průchozí nebo jsou jen příležitostně navštěvovány nebo zda jde o prostory poskytující bezprostřední přístup k bytům, kde je kladen větší důraz na soukromí obyvatelů bytů. Úřad ve Stanovisku dále uvedl místa, která mohou být kamerově sledována, aniž by byl vyžadován souhlas vlastníků či nájemníků jednotlivých bytů. Jedná se o sklepy a půdy a vchody do nich, dále garáže, kočárkárny, kolárny, prostory s dopisními schránkami a vnější plášť budovy včetně jeho bezprostředního okolí. Obvykle jsou k těmto prostorům řazeny ještě i vstupní dveře do domu, vstupní chodby k výtahům a schodištím a výtahy a schodiště samotné.

Monitorování vchodových dveří do bytů může být problematické, neboť tyto prostory mohou více vypovídat o soukromí obyvatel domu. Pokud jsou kamerově sledovány konkrétní byty, půjde zpravidla o závažný zásah do práva na ochranu soukromého a osobního života, a proto lze tyto prostory sledovat jen ve výjimečných a odůvodněných případech, a to za předpokladu, že obyvatelé dotčených bytů poskytnou souhlas s kamerovým sledováním.[76]

[75]ve znění revize z června 2018
[76] Stanovisko č. 1/2016: Umístění kamerových systémů v bytových domech, ve znění revize z června 2018

Lze si představit situaci, kdy v bytovém domě bude docházet k opakovaným krádežím či opakovanému poškozování věcí. Za účelem prevence před vandalismem se společenství vlastníků jednotek rozhodne zavést kamerový systém. Vlastníci či nájemníci bytů, kde kamera zachycuje i jejich vstup do bytu vysloví souhlas s monitorováním i tohoto prostoru, neboť jsou si vědomi, že to může přispět k dopadení pachatele.

4.3.2 Souhlas jen některých vlastníků jednotek či nájemníků

Pokud se podíváme na zákonný důvod zpracování osobních údajů, tak již víme, že zpracování osobních údajů lze provádět za předpokladu, že máme souhlas subjektu údajů nebo pokud je zde jiný zákonný důvod, kdy je zpracování údajů nezbytné. Z dikce ustanovení čl. 6 GDPR přitom plyne, že jednotlivé podmínky pro zpracování, resp. právní tituly zpracování jsou rovnocenné, kdy postačí naplnit alespoň jeden z těchto právních titulů a je jedno který. Nejužívanějším důvodem pro zpracování osobních údajů budou pravděpodobně oprávněné zájmy daného správce či třetí osoby.

V případě bytového domu, kde má být kamera umístěna tak, že zabírá i konkrétní byty, Úřad uvedl, že tak lze učinit jen výjimečně a v odůvodněných případech a se souhlasem dotčených osob.[77]

Souhlas tak bude vyžadován v případě, že mají být kamerové sledovány vchodové dveře do bytu. V těchto případech je nutné vyžádat si souhlas všech dotčených osob, jejichž byty mají být monitorovány. Naopak souhlasu nebude třeba v případech, kdy budou monitorovány ostatní prostory, jako například sklepy, půdy, garáže, kolárny, prostory schránek apod. Tedy všechny ostatní prostory s výjimkou vstupních dveří do konkrétního bytu.[78]

Z uvedeného plyne, že pokud má být zaveden kamerový systém, který bude sledovat společné prostory domu a nebude snímat vstupní dveře do konkrétního domu, lze tak učinit i na základě jiného právního titulu, než je souhlas. Může se jednat typicky o oprávněné zájmy obyvatelů domu. Pokud bude kamerový systém provozován i na základě souhlasu, pak bude SVJ či družstvo muset získat souhlas většiny svých členů.[79]

---

[77] Tamtéž, bod 6 a 7

[78] RADKOVIČOVÁ, Lucie. *Kamery v bytovém domě a právní povinnosti* [online]. radkovicova.cz, 19. července 2016 [cit. 17. července 2020]. Dostupné na <https://radkovicova.cz/2016/07/kamery-v-bytovem-dome-a-pravni-povinnosti/>.

[79] zákon č. 89/2012 Sb., občanský zákoník, § 1206 odst. 2 ve spojení se zákonem č. 90/2012 Sb., zákon o obchodních korporacích, § 645

Jestliže naopak má být zamýšlený kamerový systém namířen i na konkrétní byty, například z důvodu opakovaných útoků na majetek, pak je nezbytné získat souhlas všech takto dotčených vlastníků či nájemníků bytů.

Podmínky pro pořízení a následný provoz bezpečnostní kamery v bytovém domě jsou s ohledem na shora uvedené v některých případech přísnější. Jak uvádí Úřad v někdy je nezbytné trvat na souhlasu všech dotčených osob.[80] Obecně lze zavést kamerový systém v bytovém i domě i na základě jiného právního titulu, než je souhlas. Domnívám se však, že souhlas se zavedením kamerového systému, bez ohledu na jiný právní důvod, by měl být vyžadován i v případě, že má kamera monitorovat společné prostory jako sklepy, půdy, kolárny apod. Zamýšlená instalace kamery totiž spadá pod správu domu. Dle OZ zahrnuje správa domu vše, co je nutné a účelné pro řádnou péči o dům a pozemek, včetně zachování a zlepšení společných částí domu.[81] Do správy domu můžeme zahrnout i kontrolu nad společnými částmi domu, zejm. zda nejsou poškozovány. Tuto kontrolu pak bude vykonávat správce (nevznikli SVJ) nebo SVJ.[82] V případě SVJ, zde mohou vlastníci pověřit konkrétní osobu, která bude provádět některé úkony správy domu.[83] Záleží jen na vlastnících, které úkony této osobě svěří a které úkony podmíní svým souhlasem. Konkrétně zavedení kamerového systému není zcela jednoduchou záležitostí, naopak je s tím spojena řada povinností. Bude také třeba uzavřít smlouvu s příslušným dodavatelem a na uzavření takové smlouvy by se měli vlastníci dohodnout. Také bude třeba vynaložit určité finanční prostředky pro zavedení kamer. Domnívám se tedy, že z těchto důvodů by měl být provoz kamerového systému v jakýchkoliv částech domu postaven na souhlasu jakožto jednoho z možných zákonných titulů pro zpracování osobních údajů.

[80] Stanovisko č. 1/2016: *Umístění kamerových systémů v bytových domech*, ve znění revize červen 2018
[81] zákon č. 89/2012 Sb., občanský zákoník, § 1189
[82] NOVOTNÝ, Marek a kol. *Bytové spoluvlastnictví a bytová družstva: Komentář.* Praha: C.H. Beck, 2016. s. 413 (§ 1189)
[83] zákon č. 89/2012 Sb., občanský zákoník, § 1208 písm. g)

5 Nakládání s kamerovým záznamem

5.1 Délka uchovávání kamerového záznamu

Kamerové záznamy jsou uchovávány tak, že jsou uloženy na nosič informací. V daném případě je nosičem informací technické médium jako například harddisk počítače, DVD nebo ÚSB úložiště. V případě tabletu či telefonu jde o elektronické zařízení jehož součástí jsou nosiče dat.[84]

Zpracovávání osobních údajů je mimo výše zmíněné povinnosti limitováno také délkou uchovávání nashromážděných osobních údajů. Tomu odpovídá zásada omezeného uložení zpracovaných informací zakotvena v čl. 5 odst. 1 písm. e) GDPR. Zmíněné ustanovení je však poměrně vágní, neboť pouze uvádí, že údaje by neměly být uchovávány po dobu delší, než je nezbytné pro stanovené účely zpracování. Výjimku, z tohoto pravidla, kdy lze údaje uchovávat i po delší dobu, tvoří případy zpracování osobních údajů pro účely archivace ve veřejném zájmu, za účelem vědeckého či historického výzkumu nebo pro účely statistické. Lze si také představit použití osobních údajů například v soudním řízení. Údaje však musí být uchovávány tak, aby nedošlo k jejich použití pro jiný než stanovený účel.[85]

Jak dlouho mohou být záznamy z kamer uchovávány není jednoznačně stanoveno. Obecné nařízení ani zákon o zpracování osobních údajů na tuto otázka nedává jednoznačnou odpověď. Alespoň obecně lze říct, že tato doba bude odvislá od konkrétního účelu, pro který ke zpracování osobních údajů dochází. Přijatelnou dobou pro uchovávání záznamu bude zpravidla několik dní, popřípadě týdnu v závislosti na konkrétním provozovateli kamerového záznamu. Každý provozovatel by si tak měl být schopen odůvodnit dobu potřebnou pro uchovávání záznamu. Jakmile uplyne doba, kterou si daný provozovatel kamerového systému určí, záznam by měl být smazán. Může však nastat situace, že na záznamu bude zachycena například krádež motorového vozidla. V takovém případě přichází v úvahu prodloužení doby uchování záznamu za účelem poskytnutí součinnosti orgánům činným v trestím řízení.[86]

V případě bytového domu by dle Úřadu měly být záznamy uchovávány zpravidla nejvýše po dobu 7 dní. V případě záznamu prostor, které jsou jen příležitostně navštěvovány (např. půda, kočárkárny, sklepy), pak po dobu až 14 dní. Nicméně v odůvodněných případech mohou být záznamy uchovávány i déle.[87] Může se jednat právě o případy, kdy záznam bude třeba k prošetření nějakého incidentu.

---

[84] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. s. 116
[85] KUČEROVÁ Alena a kol. *Zákon o ochraně osobních údajů: Komentář*. Praha: C.H. Beck, 2012. 536 s.
[86] ŽŮREK Jiří. *Praktický průvodce GDPR*..., s. 220 - 221
[87] Stanovisko Úřadu č. 1/2016: Umístění kamerového systému v bytových domech, ve znění revize 2018

Stanovisko Úřadu se vztahuje na bytové domy, nicméně závěry v něm uvedené bude pravděpodobně možné vztáhnout i na vlastníky rodinných domů. Sedmidenní doba pro uchovávání záznamu se jeví i v těchto případech jako dostačující. Účelem, pro který jsou kamery zaváděny je nejčastěji ochrana majetku, života a zdraví osob. Proto i v případě rodinných domů bude jistě možné v odůvodněných případech záznam uchovávat déle než 7 dní. Lze si představit situaci, kdy se několik dní v domě nebude nikdo nacházet, typicky v případě dovolené. Pokud by v mezidobí došlo k zásahu do některého z chráněných statků a záznam byl vymazán dříve než se vlastník stačí vrátit, z tohoto pohledu by byla znemožněna identifikace pachatele. V této chvíli by se stal kamerový systém bezpředmětným.

5.2 Zabezpečení záznamu proti zneužití

Je nepochybné, že provozování bezpečnostních kamer sebou přináší řadu povinností. Výše je již objasněno, kdy dochází ke zpracovávání osobních údajů v souvislosti s provozem kamer. Tato otázka je důležitá mimo jiné proto, že zpracovávané osobní údaje o každém jednotlivém člověku je potřeba náležitě zabezpečit, aby nedošlo k jejich zneužití. Tomu odpovídá zásada zakotvena v čl. 5 odst. 1 písm. f) GDPR a sice integrita a důvěrnost. Podstata této zásady spočívá v povinnosti náležitě zabezpečit zpracovávané osobní údaje, včetně zajištění jejich ochrany vhodnými technickými či organizačními opatřeními tak, aby nedošlo k jejich neoprávněnému či protiprávnímu zpracování. Rovněž tomu odpovídá povinnost zabezpečit získané osobní údaje tak, aby nedošlo k jejich náhodné ztrátě, jejich zničení či poškození. Ke ztrátě dojde tehdy, jestliže osobní údaje sice existují, nicméně správce nad nimi již nemá kontrolu nebo k nim ztratil přístup. K poškození dojde, jestliže byly údaje změněny. Pokud údaje již vůbec neexistují nebo existují, avšak v jiné formě pro správce nepoužitelné, došlo ke zničení údajů.[88]

Zásada důvěrnosti a integrity zpracovávaných údajů je dále rozvedena v čl. 32 GDPR. Zpracovatel a správce mají povinnost zajistit takovou úroveň zabezpečení, která by odpovídala danému riziku. Je potřeba zohlednit současný stav techniky, náklady na provedení zabezpečení, povahu, rozsah, kontext a účel zpracovávaných informací a dále různě pravděpodobná a závažná rizika pro práva a svobody fyzických osob. Je zde také uveden výčet případů, jak takové zabezpečení provést, např. pseudonymizace a šifrování osobních údajů či zajištění odolnosti systému a služeb zpracování.

[88] JANEČKOVÁ, Eva. *GDPR řešení problémů v praxi obcí*. Praha: Grada Publishing, 2019. 344 s.

Lze tak vidět, že nařízení reflektuje neustálý vývoj techniky, kdy apeluje na zpracovatele, popř. správce, aby dostatečně zabezpečili systém, kde jsou ukládány osobní údaje a tím tak zamezili neoprávněnému vniknutí do příslušného sytému a tím i neoprávněnému získání, popř. použití osobních údajů.

V případě záznamu z bezpečnostních kamer je potřeba zajistit ochranu přenosových cest a datových nosičů, kam jsou záznamy ukládány, aby nemohlo dojít k neoprávněnému přístupu k nim.[89]

Je to již několik let, co pracovní skupina WP29 ve svém stanovisku shrnula požadavky na zabezpečení kamerového záznamu, nicméně závěry tam uvedené jsou použitelné i dnes. Stěžejní je zejména možnost shlédnout kamerový záznam. Přístup k danému záznamu by měl být omezený a měly by mít k němu přístup pouze konkrétně určené osoby, a to pouze za účelem, pro který se záznam pořizuje, příp. pak za účelem údržby daného systému. Jestliže je kamerový systém provozován za účelem prevence kriminality, je vhodné doporučit vytvoření dvou přístupových klíčů, kdy jeden bude mít sám provozovatel a jeden policie.[90]

V případě vytvoření dvou přístupových klíčů vyvstává otázka, zda je toto skutečně nezbytně nutné. Kamerové systémy jsou v případě bytových domů instalovány především za účelem ochrany majetku, ale také života a zdraví osob. V případě, že dojde k zásahu do některého z těchto chráněných statků a věc bude řešit policie, může využít přístupové údaje samotného provozovatele. Není tak nutné vytvářet další přístupový klíč, tím se totiž zvyšuje riziko zneužití osobních údajů. Samotné poskytnutí záznamu příslušníkům policie je také riskantním krokem z pohledu ochrany osobních údajů, avšak v praxi často nezbytný krok k prošetření celé záležitosti.

Obecně ve vztahu k povinnosti dostatečného zabezpečení lze závěrem uvést, že současná právní úprava se snaží reagovat na rostoucí hrozby v důsledku technologického rozvoje. Evropský zákonodárný orgán se snaží posílit právní mechanismy ochrany soukromí před neustále novými technologickými hrozbami.[91] Proto i v případě kamerových záznamů bude třeba přistoupit k takovému zabezpečení, které se bude jevit z pohledu současného stavu techniky dostatečným.

[89] BARTÍK, Václav, JANEČKOVÁ Eva. *Zpracovávání osobních údajů obcemi…,* s. 114-115
[90] Stanovisko č. 4/2004 WP 29 ke zpracování osobních údajů prostředky kamerového sledování
[91] BJORKLUND, Frederika, SVENONIUS, Ola. *Video Surveillance and Social Control in a Comparative Perspective*. New York: Routledge, 2013. s. 120 – 123

5.3 Další nakládání s kamerovým záznamem

Není vyloučeno, že záznam z kamery bude poskytnut třetí osobě. I takovéto nakládání s osobními údaji však musí mít základ v čl. 6 GDPR. Evropský sbor pro ochranu osobních údajů (European Data Protection Board) vypracoval stanovisko ke zpracování osobních údajů prostřednictvím videozáznamů.[92] V části 4. řeší otázku, co v případě poskytnutí záznamu třetím osobám. Jestliže má být záznam poskytnut třetí osobě pro jiný účel, než který byl stanoven pro provoz daného zařízení, je třeba naplnit požadavky čl. 6 odst. 4 GDPR. Důležité je, zda je tento jiný účel slučitelný s účelem, pro který byly osobní údaje shromážděny. Příkladem, kdy se bude jednat o slučitelný účel je situace, kdy kamerový systém byl nainstalován za účelem sledování parkoviště. Na sledovaném parkovišti došlo k poškození závory. Záznam bude předán pro účely trestního či správního řízení. Jestliže by ale takový záznam byl zveřejněn na internetu za účelem pobavení se, nejedná se již o slučitelný účel. Právní základ pro takovéto zpracování by tak dán nebyl.[93]

Závěrem je třeba ještě zmínit, že pokud třetí osoba obdrží záznam z kamery, je povinna analyzovat, zda pro zpracování osobních údajů takto získaných má i ona sama právní základ podle čl. 6 GDPR. Toto pravidlo může hrát roli zejména v případech, kdy v rámci probíhajícího řízení (ať už správního či trestního) se bude právní zástupce domáhat přístupu k danému záznamu pro hájení práv svého klienta.[94]

5.4 Následky porušení povinností při nakládání se záznamem

5.4.1 Ochrana v civilním soudním řízení

Jak je již výše uvedeno provozovatele kamerového systému tíží řada povinností, na jejichž dodržování je nutno trvat. Poměrně snadno se může stát, že některá z povinností bude porušena, ať již úmyslně či v důsledku nedbalosti provozovatele.

Neoprávněným zpracováním osobních údajů může být zasaženo do práva na soukromí člověka. Soukromí člověka patří mezi absolutní osobnostní práva a tomu odpovídá povinnost ostatních zdržet se jakýchkoliv zásahů do tohoto práva. V případě zásahu do práva na soukromí může dojít ke vzniku nemajetkové újmy, jež bývá odškodňována poskytnutím zadostiučinění. Člověk dotčený na svých právech si tak může pomoci buďto sám cestou svépomoci nebo se může domáhat ochrany u civilního soudu.[95]

[92] Guidelines 3/2019 on processing of personal data through video devices
[93] Tamtéž, str. 15
[94] Tamtéž
[95] LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1 – 654). Komentář*. Praha: C.H. Beck, 2014. s. 517-521

5.4.2 Ochrana ve správním řízení

Další prostředek ochrany poskytuje Obecné nařízení v čl. 77. Jedná se o možnost obrátit se se stížností na dozorový úřad. U nás je tímto dozorovým úřadem Úřad pro ochranu osobních údajů. Dozorový úřad může správce či zpracovatele osobních údajů například napomenout nebo uložit pokutu v přiměřené výši. V případě výše pokuty se přihlédne zejména k povaze a závažnosti porušené povinnosti, délce porušování povinností, dále povaze, rozsahu či účelu zpracovávaných informací, k počtu dotčených subjektů, míře způsobené škody a dále k zavinění (zda se jednalo o nedbalostní či úmyslné porušení povinností).[96]

Jestliže stěžovatel nebude spokojen s rozhodnutím dozorového úřadu, může proti němu podat řádný opravný prostředek, kterým je rozklad.[97]

5.4.3 Ochrana ve správním soudnictví

Může nastat situace, kdy ani v řízení o rozkladu nebude vydáno rozhodnutí, se kterým bude stěžovatel spokojen. V takovém případě je možné podat ke správnímu soudu žalobu proti rozhodnutí správního orgánu ve smyslu § 65 a násl. zákona č. 150/2002 Sb., soudní řád správní.

V případě, že se stěžovatel nejprve obrátí na dozorový úřad a tento bude nečinný, lze se rovněž domáhat ochrany svých práv žalobou u správního soudu. Bude se jednat o žalobu proti nečinnosti správního orgánu ve smyslu § 79 a násl. soudního řádu správního

5.4.4 Přestupky

Z praktického hlediska je pro provozovatele kamerového systému důležité vědět, jaké sankce jej čekají v případě porušení právních povinností při nakládání s osobnímu údaji získané pomocí záznamu z kamery.

Jednou z těch mírnějších sankcí, která může být provozovateli uložena je napomenutí či nařízení, aby zpracování údajů uvedl do souladu s Obecným nařízením.[98] Vedle těchto sankcí je však dozorový úřad oprávněn nařídit výmaz, opravu či omezení zpracování údajů, případně lze uložit i správní pokutu. [99] V případě, že dozorový úřad zvolí sankci ve formě správní pokuty, upravuje nařízení základní pravidla pro jejich ukládání. Na tomto místě je vhodné upozornit, že například za porušení povinnost provozovatele dostatečně zabezpečit systém, aby nemohlo dojít k neoprávněnému zásahu do práv a svobod fyzických osob, může být uložena pokuta až

[96] NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Nakladatelství Aleš Čeněk, 2018. s. 59 – 60
[97] zákon č. 500/2004 Sb., správní řád, § 152
[98] čl. 58 odst. 2 písm. b) a d) GDPR
[99] čl. 58 odst. 2 písm. g) a i) GDPR

do výše 10 mil. EUR.[100] Ještě vyšší je pokuta v případě nedodržení základních zásad pro zpracování osobních údajů (zejm. zákonnost zpracování a podmínky obdržení souhlasu). Dalším takovým příkladem je nedodržení příkazu dozorového úřadu spočívající v omezení zpracovávání osobních údajů. V těchto posledních dvou zmiňovaných případech hrozí pokuta až do výše 20 mil. EUR.[101]

Právní úpravu přestupků obsahuje i zákon o zpracování osobních údajů. V ustanovení § 62 zákon přejímá jednotlivé přestupky uvedené v Obecném nařízení. Vzhledem k tomu, že Obecné nařízení je přímo použitelné, není třeba implementace. Cílem úpravy v § 62 je zdůraznit, že při vyšetřování přestupků bude Úřad postupovat podle zákona o odpovědnosti za přestupky.[102]

Sankce, které hrozí při porušení povinností stanovených Obecným nařízení jsou velice vysoké a mohou být až likvidačního charakteru. Cílem je uložit takovou sankci, aby byla dostatečně účinná a odrazující, ale zároveň aby byla v přiměřené výši. Při stanovování její výše se bude přihlížet hned k několika aspektům v závislosti na konkrétním případě. Výše jsem již uvedla příklady, k jakým okolnostem se bude přihlížet, kromě tedy povahy a závažnosti porušení povinnosti, účelu a rozsahu zpracovávaných informací, počtu dotčených subjektů se bude zohledňovat i to, jak se Úřad dozvěděl o porušení povinnosti (zda tuto skutečnost provozovatel sám oznámil či nikoli), zda se jedná o prvotní porušení povinností nebo například k tomu, jaké osobní údaje byly dotčeny.[103]

Správní pokuty dosahující až milionových částek jsou s největší pravděpodobností odůvodněny závažnosti dotčených práv a svobod fyzických osob. Zpracováním osobních údajů dochází totiž k zásahu do soukromí jednotlivce. Jak už je v této práci uvedeno, soukromí člověka patří mezi absolutní práva, čemuž odpovídá povinnost všech ostatních zdržet se jakýchkoliv zásahů do této sféry. Je to jedno ze základních lidských práv, a proto je třeba důsledně trvat na tom, aby tato práva nebyla nikterak porušována, aby nedocházelo k neoprávněným zásahům. V drtivé většině případů bude provozováním bezpečnostních kamer docházet ke zpracování osobních údajů, a proto je nezbytné, aby i provozovatelé kamerových systémů důsledně dbali na dodržování obecných pravidel pro zpracování osobních údajů.

[100] čl. 83 odst. 4 písm. a) GDPR
[101] čl. 83 odst. 5 písm. a) a e) GDPR
[102] VLACHOVÁ, Barbora, MASISNER, Martin. *Zákon o zpracování osobních údajů. Komentář*. Praha: C.H. Beck 2019. 268 s.
[103] čl. 83 odst. 1, odst. 2 GDPR

5.4.5 Trestné činy

Je potřeba pamatovat i na to, že porušení povinností při zpracovávání osobních údajů může mít své důsledky i v trestněprávní rovině. Trestní zákoník upravuje hned několik trestných činů v této oblasti. Pro účely této diplomové práce je na místně zmínit trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací ve smyslu § 230 trestního zákoníku. Základní skutková podstata tohoto trestného činu spočívá v překonání bezpečnostního opatření, a tím neoprávněného získání přístupu k počítačovému systému či k jeho části. Druhá základní skutková podstata spočívá v získání přístupu k počítačovému systému nebo k nosiči informací a neoprávněného užití dat takto získaných, vymazání či poškození dat, padělání či pozměnění dat nebo neoprávněného vložení dat do počítačového systému či nosiče informací.

Počítačovým systémem může být jakékoliv zařízení či skupina vzájemně propojených zařízení, kde dochází k automatickému zpracování dat. Nosičem informací je pak například pevný disk počítače, kompaktní disk, DVD apod, tedy cokoliv, na čem lze zaznamenávat údaje a tyto údaje pak znovu získat. Zároveň je zde podmínka, že pachatel musí překonat bezpečnostní opatření.[104]

S ohledem na uvedené definice je zřejmé, že i neoprávněné získání přístupu ke kamerovému systému a jeho záznamu může naplnit skutkovou podstatu výše uvedeného trestného činu. Podmínka překonání bezpečnostního opatření pachatele v první základní skutkové podstatě reaguje na povinnost provozovatele kamerového systému dostatečně zabezpečit systém tak, aby nemohlo dojít k jeho zneužití. Jestliže provozovatel kamery tuto povinnost poruší a pachatel získá volný přístup ke kamerovému systému, včetně jeho záznamu bude naplněna druhá základní skutková podstata tohoto trestného činu. Vedle toho zde pak bude odpovědnost provozovatele v rovině správní, který porušil povinnost uloženou mu Obecným nařízením. Více k odpovědnosti provozovatele je uvedeno v předchozí podkapitole.

Někdy může být obtížné rozeznat, kdy se jedná o odpovědnost v rovině správní a kdy v rovině trestní. Kritériem odlišení bude zásada subsidiarity trestní represe zakotvena v § 12 trestního zákoníku. Podstata této zásady spočívá v tom, že trestněprávní odpovědnost a důsledky z ní plynoucí se uplatní až v případech společensky škodlivých, kdy nepostačuje uplatnění odpovědnosti dle jiného právního předpisu. Čili pokud zde postačí uplatnění odpovědnosti za přestupek, pak není namístě posuzovat odpovědnost v rovině trestněprávní.[105]

[104] JELÍNEK, Jiří a kol. *Trestní zákoník a trestní řád s poznámkami a judikaturou*. 6. vydání. Praha: Leges, 2016. s. 347 -349
[105] MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012. s 195

6 Vliv GDPR na užívání bezpečnostních kamer

V této kapitole se zaměřím na nejdůležitější změny, které s sebou Obecné nařízení přineslo. GDPR nemělo příliš extrémní vliv na používání bezpečnostních kamer z pohledu ochrany osobních údajů v tom smyslu, že by zcela změnilo základní podmínky pro instalaci a následný provoz bezpečnostních kamer. To však neznamená, že se nová právní úprava ochrany osobních údajů nijak nedotkla provozování kamerových systémů. Určité změny v této oblasti nastaly a nyní proto zmíním ty, které považuji z praktického hlediska za nejzásadnější.

6.1 Oznamovací povinnost

Dříve než vešlo v platnost Obecné nařízení, byl provozovatel kamerového systému povinen písemně oznámit svůj záměr Úřadu. Nejprve tedy bylo potřeba oznámit Úřadu, že provozovatel hodlá zavést kamerový systém, kde bude docházet ke zpracovávání osobních údajů. Teprve až po uplynutí 30 dnů ode dne doručení oznámení Úřadu mohl provozovatel začít provozovat kamerový systém. Stejně tak v případě, že provozovatel porušoval podmínky stanovené zákonem, mohl mu Úřad registraci zrušit, což pro provozovatele znamenalo ukončení provozování kamerového systému.[106] To vše za předpokladu, že při provozování kamery docházelo ke zpracování osobních údajů.

Oznamovací povinnost byla zavedena za účelem kontroly dozorového úřadu. Splněním oznamovací povinnost byl zveřejněn účel zpracování a základní vlastnosti takovéhoto zpracování. Úřad pak mohl kontrolovat soulad zpracovávání osobních údajů s právními předpisy a v případě nesouladu, mohl zamezit takovémuto zpracování.[107]

Od 25. května 2018 tato povinnost odpadla. V současné době již není třeba hlásit Úřadu zamýšlenou instalaci kamerového systému, při němž bude docházet ke zpracování osobních údajů. To však neznamená, že provozovatelé nebudou dozorování ze strany Úřadu. Naopak přibyla jim řada nových povinností.[108]

Jednou z těchto nových povinností je vypracování analýzy, kde vyhodnotí vliv kamerového systému na ochranu osobních údajů. V rámci této analýzy je třeba zhodnotit nezbytnost a přiměřenost monitorování, dále je třeba posouzení rizik pro práva a svobody osob

[106] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, § 16 a § 17
[107] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související. Komentář*. Praha: Wolters Kluwer, 2014. s. 249 – 250
[108] VEJVODOVÁ, Alžběta. Kamery už se nemusí hlásit státu. Veškerá odpovědnost se přesouvá na provozovatele. [online]. pravniradce.ihned.cz, 19. června 2018 [cit. 30. června 2020]. Dostupné na <https://pravniradce.ihned.cz/c1-66173030-kamery-se-uz-nemusi-hlasit-statu-veskera-odpovednost-se-presouva-na-jejich-provozovatele >.

zachycených na záznamu. Provozovatel musí také uvést, jaká přijal bezpečnostní opatření k ochraně dat, případně jaká plánuje zavést.[109]

Posouzení vlivu ve smyslu čl. 35 GDPR se má provést zejména v situacích, kdy dojde k využití nových technologií, kdy zpracování osobních údajů bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob. Toto posouzení je třeba provést, ještě před započetím zpracování. Zpočátku bylo nejasné, zda bude tato povinnost dopadat i na provozovatele kamerového systému.[110] Následně tuto otázku vyřešil Úřad, když vydal dokument, kde uvádí, které operace budou podléhat posouzení vlivu na ochranu osobních údajů a které nikoli. Podle tohoto dokumentu je první skupinou podléhající posouzení vlivu zpracovávání zahrnující monitorování subjektů. Zde spadají tři okruhy případů, kdy subjekty údajů musí být identifikovatelné/identifikované a 1) lokalizovatelné, 2) rozpoznatelné či 3) jinak monitorované. Přičemž běžný kamerový systém spadá pod druhý okruh případů.[111]

Stále však zůstává otázka, zda se tato povinnost vztahuje na všechny provozovatele kamerového systému. Obecné nařízení hovoří o této povinnost v souvislosti s možným vysokým rizikem pro práva a svobody fyzických osob. [112] Míra rizika zásahu do práva a svobod lidí bude pravděpodobně odlišná v případě kamerového systému bytového domu a v případě kamery umístěné na rodinném domě. U bytového domu může docházet ke zpracování osobních údajů až několik desítek osob, a to nejen jednotlivých vlastníků či nájemníků, ale i jiných osob, které se tam příležitostně pohybují. Naproti tomu u rodinného domu umístěného na konci klidné ulice nebude pohyb osob příliš častý (nepočítaje obyvatelé domu). Je nutné vyžadovat pak i od těchto osob vypracování posouzení vlivu? Zde se domnívám, že nikoli. A to právě s ohledem na to, že v tomto případě nebude vysoké riziko zásahu do práv a svobod fyzických osob, neboť ve srovnání s bytovým domem nebude zpracováno tolik osobních údajů.

6.2 Nová práva a povinnosti

6.2.1 Záznamy o činnostech

Obecné nařízení zavedlo povinnost vést záznamy o činnostech zpracování. Provozovatelé za tyto záznamy odpovídají a jsou povinni je vést v písemné formě a na požádání je poskytnout

[109] čl. 35 GDPR
[110] KUČEROVÁ, Alena. *GDPR – kamery v bytovém domě v roce 2018*. [online]. tzb-info.cz, 5. 6. 2017 [cit. 30. června 2020]. Dostupné na < https://www.tzb-info.cz/kamerove-systemy/15861-gdpr-kamery-v-bytovem-dome-v-roce-2018>.
[111] Seznam druhů operací zpracování (ne)podléhající požadavku na posouzení vlivu na ochranu osobních údajů. Dostupné na < https://www.uoou.cz/povinnosti-spravcu/ds-5856/archiv=0&p1=3938 >.
[112] čl. 35 odst. 1 GDPR

Úřadu. Obecné nařízení stanoví obsahové náležitosti těchto záznamů. Zejména je třeba, aby záznamy obsahovaly kontaktní údaje správce, účel zpracování, jaké osobní údaje a jakých subjektů jsou zpracovávány, lhůty pro výmaz a popis bezpečnostních opatření.[113]

Dá se říct, že tato nová povinnost do jisté míry kompenzuje zrušení oznamovací povinnosti o zamýšleném zavedení kamerového systému, kde bude docházet ke zpracování osobních údajů. V čase, kdy provoz kamerového systému byl postaven na registračním principu, mohl Úřad zhodnotit, zda jsou dodrženy všechny zákonem stanovené náležitosti. Jestliže však Úřad zjistil, že oznámené zpracování osobních údajů není v souladu se zákonem, zpracování, a tedy provoz kamerového systému, nepovolil.[114]

Poté, co vstoupilo v platnost GDPR, již nemusí provozovatelé oznamovat zamýšlenou instalaci kamerového systému a Úřad tak nemá možnost předem posoudit oprávněnost takovéhoto zpracování osobních údajů. Naproti tomu však díky nově zavedené povinnosti vést záznamy, muže provést kontrolu alespoň tímto způsobem, kdy si vyžádá písemnou zprávu o vedení záznamu. Toto však není jediná možnost, jak může úřad dohlížet na zpracovávání osobních údajů. Například v předchozí podkapitole jsem uvedla povinnost posouzení vlivu na zpracování osobních údajů s ohledem na možná rizika zásahu do práv a povinností lidí.

6.2.2 Ohlašování případů porušení zabezpečení osobních údajů

Samotná otázka zabezpečení osobních údajů je řešena v kapitole páté této práce. Na tomto lze ještě uvést, že bezpečné nakládání s osobními údaji má za následek nejen bezpečnost samotných dat, ale i bezpečnost subjektů údajů, resp. jejich soukromí. Pokud budou přijata dostatečná bezpečnostní opatření, minimalizuje se tím hrozba zásahu do soukromí, což je také primární účel právní úpravy.[115]

Se zabezpečením osobních údajů souvisí další novinka mezi povinnostmi správce, a sice ohlášení Úřadu jakékoliv porušení zabezpečení osobních údajů, a to do 72 hodin od okamžiku, kdy se o tom správce dozvěděl. Výjimkou jsou situace, kdy je nepravděpodobné, že by tímto porušením vzniklo riziko pro práva a svobody fyzických osob.[116]

Bude se jednat zejména o případy, kdy se kamerový záznam dostane na veřejnost nebo se dostane do rukou neoprávněné osoby.

---

[113] čl. 30 GDPR
[114] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, § 17
[115] BARTÍK, Václav, JANEČKOVÁ, Eva. Bezpečnost osobních údajů podle zákona o ochraně osobních údajů. *Právní rozhledy*, 2010, č. 23, s. 839 – 840
[116] čl. 33 GDPR

Vedle oznamovací povinnosti vůči Úřadu má správce rovněž oznamovací povinnost vůči subjektu údajů. Tuto povinnost musí správce splnit v případě, že v důsledku porušení zabezpečení osobních údajů vznikne vysoké riziko zásahu do práv a svobod subjektů. I z této oznamovací povinnosti jsou výjimky. První výjimkou jsou případy, kdy správce provede šifrování, kdy údaje neoprávněně získané se stanou nesrozumitelnými. Dále není třeba oznámení, pokud správce přijal opatření snižující vysoké riziko zásahu do práv a svobod. Nakonec se jedná situace, kdy oznámení by znamenalo nepřiměřené úsilí, musí však svou oznamovací povinnost splnit jiným způsobem, například veřejným oznámením.[117] Poslední výjimka bude patrně dopadat na situace, kdy v důsledku překonání zabezpečení unikne velké množství osobních údajů mnoha subjektů. Tady je zřejmé, že pokud by měl správce obeznámit každý jednotlivý subjekt zvlášť, bylo by to velmi náročné. Proto může svou oznamovací povinnost splnit hromadným veřejným oznámením.

6.2.3 Právo na výmaz

Kromě řady povinností zavedlo Obecné nařízení i řadu nových práv. Mezi ně patří i právo na výmaz neboli „právo být zapomenut“. Obsahem tohoto práva je požadovat po správci vymazání osobních údajů týkající se daného subjektu. Správce tak musí učinit bez zbytečného odkladu. Subjekt údajů však musí odůvodnit, proč tak žádá. Nařízení uvádí několik důvodů na základě, kterých může subjekt údajů uplatnit právo být zapomenut. Jedná se zejména o případy, kdy subjekt odvolal souhlas se zpracováním osobních údajů, osobní údaje již nejsou potřebné pro účely, za kterými byly shromážděné nebo například byly zpracovány protiprávně. [118]

Obecné nařízení pak uvádí v čl. 17 odst. 3 případy, kdy se právo na výmaz neuplatní. Bude se jednat především o všechna zpracování osobních údajů založena na kvalifikovaném právním titulu podle čl. 6 a 9 GDPR. Pokud se jedná o provozovatele kamerového systému, tak ve chvíli, kdy obdrží žádost o vymazání osobních údajů konkrétního člověka ze záznamů, bude muset přezkoumat test proporcionality provedený již v době instalace systému. Pokud vyhoví žádosti o výmaz, pak tak učiní bez zbytečného odkladu a v souladu s čl. 12 odst. 3 o tom informuje žadatele. Jestliže naopak žádosti nevyhoví, pak bude postupovat dle čl. 12 odst. 4 a informuje žadatele nejen o tom, že jeho žádosti nevyhověl, ale také o možnosti podat stížnost u Úřadu. Provozovatel kamerového systému pak musí být připraven obhájit toto své jednání u

[117] čl. 34 GDPR
[118] čl. 17 GDPR

dozorového Úřadu. Důvodem pro odmítnutí žádosti na výmaz může být oprávněný zájem na uchování kompletních záznamů.[119]

V praxi si lze představit situaci, kdy z obytného domu bude zcizeno jízdní kolo vlastníka jednotky. Záznam tak bude třeba pro identifikaci pachatele. Pokud by ale došlo k odstranění částí záznamu, mohlo by dojít k poškození záznamu jako celku. Identifikace pachatele by pak byla nemožná či min. obtížně proveditelná a účel, pro který byl kamerový systém zaveden by byl těžko naplnitelný.

Právo na výmaz je nepochybně jedním z důležitých práv, které Obecné nařízení subjektům údajů přiznává. Vzhledem k výše uvedenému je však otázkou, zda v praxi bude toto právo ve vztahu ke kamerovým záznamům skutečně naplněno. Přece jen jde o vymazání části záznamu a provozovatelé mohou argumentovat reálným poškozením zbytku záznamu a tím případné nemožnosti využití takového záznamu v případě zásahu do některého chráněného statku. Zároveň mají provozovatelé povinnost záznamy uchovávat pouze po dobu nezbytně nutnou, což bude zpravidla 7 až 14 dní. Poté bude záznam vymazán, a to ať již automaticky v důsledku naplnění kapacity disku nebo manuálně. Osobní údaje subjektů zachycených na záznamech tedy budou vymazány tak jako tak. Odlišný bude časový okamžik, kdy se stane. Nicméně každý případ bude individuální a vždy bude záležet na okolnostech toho kterého případu. Někdy může být na místě toto právo uplatnit, jindy se to může jevit nadbytečným, a to právě s ohledem na délku uchovávání záznamu.

[119] KUČEROVÁ, Alena. *Práva subjektu údajů podle GDPR – hrozba pro provozovatele kamerových systémů II. – Právo na výmaz.* [online]. tzb-info.cz, 11. 6. 2018 [cit. 30. června 2020]. Dostupné na <https://www.tzb-info.cz/normy-a-pravni-predpisy-facility-management/17479-prava-subjektu-udaju-podle-gdpr-hrozba-pro-provozovatele-kamerovych-systemu-ii-pravo-na-vymaz >.

Závěr

Cílem mé diplomové práce bylo analyzovat podmínky pro použití bezpečnostních kamer, kdy jsem si položila otázku, *jakým způsobem je zabezpečena ochrana osobních údajů získaných z kamerových záznamů konkrétních subjektů*, tedy v případě bytových domů SVJ či družstvem, případně jednotlivců, kdy se kamera nachází na rodinném domě. Další otázkou bylo, zda *je tato ochrana dostatečná*, přičemž jsem došla k následujícím závěrům.

Nejprve bylo třeba seznámit se právní úpravou dopadající na oblast ochrany osobních údajů a také charakterizovat základní pojmy týkající se ochrany osobních údajů. Toto jsem považovala za nezbytné, jelikož kamerové systémy nejen, že jsou spjaty s ochranou soukromí, ale zahrnují i zpracování osobních údajů. Co se týče právní úpravy, hlavním pramenem práva pro oblast ochrany osobních údajů je Obecné nařízení, proto jsem mu také věnovala samostatnou podkapitolu. Základem bylo ujasnit si otázku aplikace GDPR na národní úrovni. Zde jsem došla k jednoznačnému závěru, že toto nařízení je přímo účinné a není vyžadována implementace tohoto předpisu do národního právního řádu. Navíc má toto nařízení aplikační přednost. To znamená, že v případě rozporu s vnitrostátní právní úpravou, aplikujeme Obecné nařízení. Nejedná se o zrušení právního předpisu jako takového, pouze se ponechá stranou a aplikuje se evropská právní úprava.

Pokud bych měla shrnout charakteristiku základních pojmů týkajících ochrany osobních údajů, pak zde mohu říct, že GDPR definuje základní pojmy velmi široce. Pozornost je potřeba zaměřit především na pojem osobní údaj. Stejně jako ostatní pojmy, je i pojem osobní údaj definován velmi široce. Důvodem bude skutečnost, že cílem právní úpravy ochrany osobních údajů je přispět k ochraně soukromí dotčených osob. I samotný pojem soukromí je obsáhlý pojem, který nelze odbýt jednoduchou definicí, proto je potřeba ponechat dostatečný prostor pro obsah pojmu osobní údaj.

V druhé kapitole jsem se zabývala pořizováním záznamu. Nejdříve jsem uvedla zásady zpracování osobních údajů. Na tomto místě bych ráda zdůraznila, že je skutečně nutno trvat na dodržování uvedených zásad, které považuji za základní stavební kámen pro jakékoliv zpracování osobních údajů, tedy nejen v případě kamerových záznamů. Nadto i samo nařízení stanoví odpovědnost správce za nedodržování těchto zásad, čímž zdůrazňuje jejich důležitost a nezbytnost.

Druhá kapitola mé práce se zaobírá také legitimním účelem pro zpracování osobních údajů. Každý, kdo zamýšlí zavést kamerový systém si musí nejprve položit otázku, proč tak chce učinit. Jednou z podmínek pro provozování kamerového systému je totiž legitimní účel.

V této části jsem vedla rozhodnutí soudů, které řešily případ, kdy nebyla dodržena některá z podmínek pro provoz bezpečnostní kamery, přesto však mohl kamerový záznam posloužit pro účely dokazování. Zde bych ráda zdůraznila právní názor soudů, se kterým se plně ztotožňuji, a sice, že v případě nedodržení všech podmínek, nelze postupovat čistě formalisticky, ale je potřeba zohlednit právě otázku legitimního cíle, který bychom měli zohlednit vždy v každém konkrétním případě. Každý případ je totiž individuální a k tomu je tak třeba i přistupovat. V každém jednotlivém případě mohou hrát roli různé okolnosti, které "ospravedlní" proč nebyly dodrženy všechny podmínky.

Další část práce se zaobírá otázkou, a sice zda při provozování kamerového systému dochází ke zpracování osobních údajů fyzických osob. O osobní údaje se bude jednat tehdy, když na základě záznamu z kamery budeme schopni, byť i nepřímo, identifikovat konkrétní fyzickou osobu. Tento závěr odpovídá účelu, pro který jsou kamery zaváděny. Důvodem pro zavedení kamerového systému bývá nejčastěji ochrana života, zdraví a majetku osob, ať už se jedná o prevenci před zásahy do těchto chráněných statků či k následné identifikaci pachatele. K identifikaci pachatele by však nemohlo dojít, pokud by kamera nezaznamenala žádný osobní údaj dané osoby. Stejný závěr zastává i NSS.[120] Tudíž ke zpracování osobních údajů při provozu kamery bude docházet téměř vždy. Závěrem bych ještě dodala, že je třeba pamatovat i na to, že kamery plní i funkci preventivní, kdy mají potenciálního pachatele odradit od protiprávního jednání. To však nemění nic na tom, že aby mohla kamera posloužit svému účelu, musí být schopna pachatele, byť i potenciálního, identifikovat na základě jeho osobních údajů.

Obecně každé zpracování osobních údajů musí být zákonné. Nejčastějším zákonným důvodem pro zpracování bude ochrana zájmů jednotlivce či souhlas s takovým zpracováním. Problematická se jevila otázka souhlasu, tudíž je jí vyčleněna samostatná kapitola. Zde bych ráda připomněla otázku souhlasu u bytových domů. V praxi si lze těžko představit, že v domě budou naprosto všichni souhlasit. Už jen z toho důvodu, že souhlas je odvolatelný. Pokud má kamera v odůvodněných případech zabírat i vchod do některých bytů, je třeba souhlasu dotčených vlastníků jednotek. Závěry Úřadu týkající se problematiky souhlasu mě vedly k zamyšlení se, zda v případě bytových domů není na místě vyžádat si souhlas s pořízením si bezpečnostní kamery vždy. Mé úvahy směřovaly ke správě domu dle OZ, kde jsem došla k závěru, že i záměr pořídit si kameru spadá mezi činnosti zahrnující správu domu. Zavedení kamerového systému není zcela jednoduchou záležitostí. Naplnění podmínek pro provoz kamer chvíli ponechme stranou a zaměřme se na jiné praktické otázky. Nejdříve je třeba získat, resp.

[120] rozsudek NSS ze dne 25. února 2015, sp. zn. 1 As 113/2012, bod 37

vyčlenit určité finanční prostředky na pořízení si příslušného kamerového systému, následně je třeba uzavřít smlouvu s dodavatelem, který poskytne a nainstaluje kamery. Proto jsem toho názoru, že na takových úkonech by se měli vlastníci bytů dohodnout a správce domu by tak neměl činit bez vědomí, resp. souhlasu jednotlivých vlastníků bytů.

Z praktického hlediska byla důležitá otázka, které prostory mohou být monitorovány. V případě rodinných domů bylo judikováno, že do jisté míry a za určitých okolností je přípustné zabírat i část veřejné ulice. Nicméně jasná hranice nebyla určena. Takovou hranici ani nelze jednoznačně určit, neboť každý případ je svým způsobem specifický a k tomu je třeba též přihlížet. V případě bytového domu je však situace o něco jasnější. Zde Úřad uvedl, které prostory mohou být snímány a které naopak nikoli. Od toho se pak odvíjí i délka uchovávání záznamu, obecně platí 7denní doba pro uchování záznamu. Jestliže jde o prostor méně navštěvovaný, např. sklep, je přípustná i 14denní doba. Co se týče samotné délky uchovávání záznamu, který uvedl Úřad, s jeho závěry jsem se ztotožnila. To však neznamená, že v odůvodněných případech nemůže být délka uchovávání záznamu odlišná.

Nelze opomenout ani informační povinnost provozovatele kamery. Právní úprava vyžaduje konkrétní náležitosti, které musí být splněny, aby mohla být informační povinnost řádně splněna. Dle mého názoru, by informační cedule neměla být příliš zahlcena informacemi. Naopak v každém případě kamerového snímání by postačovalo uvést, že je daný prostor monitorován, typicky pomocí obrázku kamery doplněného o stručný popis „*Tento prostor je monitorován*.“ Dále by informační cedule měla obsahovat kontaktní údaje správce. Ve zbytku jsem přesvědčena, že stačí odkázat, kde může subjekt údajů získat ostatní informace.

V další části práce zaměřila na povinnost provozovatele dostatečně zabezpečit systém před možným zneužitím záznamu, jeho ztrátě či poškozením. Provozovatel by měl přistoupit k takové formě zabezpečení, která bude odpovídat současnému stavu techniky. Abychom mohli hovořit o dostatečném zabezpečení, nejprve je třeba, aby k záznamu měl přístup pouze omezený, úzký okruh osob. Nesmí docházet ke zveřejňování záznamu na internetu ani ke svévolnému rozesílání takového záznamu dalším osobám. Pokud je kamerový systém veden za účelem prevence před kriminalitou, některé zdroje uvádějí, že je vhodné vytvořit 2 přístupové klíče pro provozovatele a policii. Toto doporučení mě vedlo k zamyšlení se, zda je to skutečně nezbytné. Domnívám se, že nikoli. Pokud by skutečně došlo k nějakému protiprávnímu jednání, kdy by věc řešila policie, postačí, pokud se k záznamu dostane přes přístupové údaje provozovatele. Tudíž bych nedoporučovala vytvářet několik přístupových klíčů.

V kapitole šesté této práce jsem se zaměřila na některé z mého pohledu nejzásadnější změny, které GDPR s sebou přineslo. S jistotou lze říct, že GDPR rozhodně neotřáslo

v základech užívání bezpečnostních kamer z pohledu ochrany osobních údajů. Na druhou stranu to však neznamená, že určité změny nenastaly. Proto jsem část práce věnovala i této problematice.

Po prostudování vybrané problematiky jsem dospěla k závěru, že ochrana osobních údajů získaných kamerovým záznamem bytových domů je zabezpečena hned několika způsoby, a to už od samotného stanovení si legitimního cíle pro zavedení kamery až po povinnost dostatečného zabezpečení získaných záznamů a omezené možnosti nakládání se záznamem. Jak lze v této práci vidět, způsobů je hned několik.

Pokud se jedná o druhou výzkumnou otázku, pak lze uvést, že ochrana osobních údajů získaných kamerovými záznamy bytových domů je poskytována dostatečně. Obecné nařízení klade přísné podmínky na provozovatele kamer a jejich nedodržení velmi znatelně sankcionuje.

S ohledem na shora uvedené mohu konstatovat, že má hypotéza, že *provoz bezpečnostních kamer je doprovázen množstvím podmínek, jejichž naplnění je nutné pro to, aby získané osobní údaje byly dostatečně chráněny*, byla potvrzena. V jistých odůvodněných případech je možné sice odhlédnout od toho, že některá z podmínek pro provoz kamery nebyla zcela naplněna, avšak na druhé straně jsou kladeny přísné požadavky na nakládání s již získanými osobními údaji. O sankcích za porušení povinností, pak ani nemluvě. Ty jsou samy o sobě dostatečně motivující pro řádné dodržování stanovených podmínek.

Bibliografie

Odborná literatura

1. BARTÍK, Václav, JANEČKOVÁ Eva. *Zákon o ochraně osobních údajů s komentářem*. Olomouc: Anag, 2010. 383 s.

2. PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR): Data a soukromí v digitálním světě: Komentář*. Praha: Leges, 2018. 488 s.

3. NULÍČEK, Michal a kol. *GDPR/Obecné nařízení o ochraně osobních údajů: Komentář*. 2. vydání. Praha: Wolters Kluwer ČR, 2018, 580 s.

4. MELZER, Filip, TÉGL, Petr a kol. *Občanský zákoník – velký komentář. Svazek I. § 1 – 117*. Praha: Leges, 2013. 720 s.

5. KUČEROVÁ Alena a kol. *Zákon o ochraně osobních údajů: Komentář*. Praha: C.H. Beck, 2012. 536 s.

6. ŽŮREK Jiří. *Praktický průvodce GDPR*. 2. vydání. Olomouc: Anag, 2018. 344 s.

7. BARTÍK, Václav, JANEČKOVÁ Eva. *Zpracovávání osobních údajů obcemi. Vybrané problémy*. Praha: Wolters Kluwer, 2013. 184 s.

8. LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1 – 654). Komentář*. Praha: C.H. Beck, 2014. 2400 s.

9. NAVRÁTIL, Jiří a kol. *GDPR pro praxi*. Plzeň: Nakladatelství Aleš Čeněk, 2018. 339 s.

10. JELÍNEK, Jiří a kol. *Trestní zákoník a trestní řád s poznámkami a judikaturou*. 6. vydání. Praha: Leges, 2016. 1280 s.

11. MATES, Pavel a kol. *Ochrana osobních údajů*. Praha: Leges, 2012. 208 s.

12. MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. 152 s.

13. NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související. Komentář*. Praha: Wolters Kluwer, 2014. 504 s.

14. VLACHOVÁ, Barbora, MASISNER, Martin. *Zákon o zpracování osobních údajů. Komentář*. Praha: C.H. Beck 2019. 163 s.

15. JANEČKOVÁ, Eva. *GDPR řešení problémů v praxi obcí*. Praha: Grada Publishing, 2019. 344 s.

16. SLÁDEČEK, Vladimír a kol. *Ústava České republiky, Komentář*. 2. vydání. Praha: C. H. Beck, 2016. 1264 s.

17. TZANOU, Maria. *Personal Data Protection and Legal Developments in the European Union*. UK: Keele University, 2020. 375 s.

18. CUSTERS, Bart and others. *EU Personal Data Protection in Policy and Practise*. The Netherlands: T.M. C. Asser Press, 2019. 249 s.

19. BJORKLUND, Frederika, SVENONIUS, Ola. *Video Surveillance and Social Control in a Comparative Perspective*. New York: Routledge, 2013. 232 s.

20. MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana.* 2. vydání. Praha: ASPI, 2008. 456 s.

21. TOMÁŠEK, Michal a kol. *Právo Evropské unie.* Praha: Leges, 2013. 496 s.

22. WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod: Komentář*. 3. vydání. Praha: Wolters Kluwer, 2012. 931 s.

23. NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: Komentář*. Praha: Wolters Kluwer, 2014. 504 s.

24. NOVOTNÝ, Marek a kol. *Bytové spoluvlastnictví a bytová družstva: Komentář.* Praha: C.H. Beck, 2016. s. 413

Odborné časopisy

1. NULÍČEK, Michal a kol. GDPR v otázkách a odpovědích. *Bulletin advokacie*, 2017, č. 9, s. 33.

2. BARTÍK, Václav, JANEČKOVÁ, Eva. Bezpečnost osobních údajů podle zákona o ochraně osobních údajů. *Právní rozhledy*, 2010, č. 23, s. 839 – 840

Právní předpisy

1. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

2. Vyhláška č. 120/1976 Sb., o Mezinárodním paktu o občanských a politických právech

3. Sdělení č. 209/1992 Sb., federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících

4. Úmluva č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních údajů

5. Smlouva o Evropské unii

6. Smlouva o fungování Evropské unie

7. Listina základních práv Evropské unie

8. Nařízení Evropského parlamentu a Rady (ES) 45/2001 ze dne 18. prosince 2000, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů

9. Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikací)

10. Ústavní zákon č. 1/1993 Sb., Ústava České republiky

11. Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky

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

13. Zákon č. 90/2012 Sb., zákon o obchodních korporacích, ve znění pozdějších předpisů

14. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

15. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

16. Zákon č. 110/2019 Sb., o zpracování osobních údajů

17. Zákon č. 500/2004 Sb., správní řád

18. Zákon č. 150/2002 Sb., soudní řád správní

19. Zákon č. 256/2013 Sb., katastrální zákon

Judikatura

1. Rozsudek Nejvyššího správního soudu ze dne 3. května 2017, sp. zn. 7 As 36/2017

2. Rozsudek Nejvyššího správního soudu ze dne 18. listopadu 2011, sp. zn. 2 As 45/2010

3. Rozsudek Nejvyššího správního soudu ze dne 23. srpna 2018, sp. zn. 5 As 158/2012

4. Rozsudek Nejvyššího správního soudu ze dne 25. února 2015, sp. zn. 1 As 112/2012

5. Usnesení Nejvyššího správní soudu ze dne 20. března 2013, sp. zn. 1 As 113/2012

6. Usnesení Nejvyššího správního soudu ze dne 22. prosince 2014, sp. zn. 1 As 113/2012

7. Rozsudek ze dne 11. prosince 2014, *Ryneš v. Úřad pro ochranu osobních údajů*, C-212/13, bod 35

8. Rozsudek Nejvyššího správní soudu ze dne 8. června 2016, sp. zn. 3 As 118/2015

9. Rozsudek Nejvyššího správního soudu ze dne 20. prosince 2017, sp. zn. 10 As 245/2016

10. Rozsudek Nejvyššího správního soudu ze dne 20. září 2017, sp. zn. 2 As 140/2017

11. Rozsudek Nejvyššího správního soudu ze dne 22. srpna 2019, sp. zn. 284/2018

12. Rozsudek ze dne 4. května 2000, *Rotaru v. Romania*, C 28341/95, bod 44

13. Rozsudek ze dne 8. dubna 1976, *Defrenne v Sabena, C* 47/75

14. Rozsudek ze dne 5. února 1963, Van Gend en Loss, C 26/62

Internetové zdroje

1. HRUŠKA, Vít. *Právní úprava kamerových systémů podle GDPR*. [online]. maceklegal.cz, 5. září 2017 [cit. 4. března 2020]. Dostupné na <https://www.maceklegal.cz/pravni-uprava-kamerovych-systemu-podle-gdpr.html>.

2. VEJVODOVÁ, Alžběta. *Kamery už se nemusí hlásit státu. Veškerá odpovědnost se přesouvá na provozovatele*. [online]. pravniradce.ihned.cz, 19. června 2018 [cit. 30. června 2020]. Dostupné na <https://pravniradce.ihned.cz/c1-66173030-kamery-se-uz-nemusi-hlasit-statu-veskera-odpovednost-se-presouva-na-jejich-provozovatele >.

3. KUČEROVÁ, Alena. *GDPR – kamery v bytovém domě v roce 2018.* [online]. tzb-info.cz, 5. 6. 2017 [cit. 30. června 2020]. Dostupné na <https://www.tzb-info.cz/kamerove-systemy/15861-gdpr-kamery-v-bytovem-dome-v-roce-2018>.

4. KUČEROVÁ, Alena. *Práva subjektu údajů podle GDPR – hrozba pro provozovatele kamerových systémů II. – Právo na výmaz*. [online]. tzb-info.cz, 11. 6. 2018 [cit. 30. června 2020]. Dostupné na <https://www.tzb-info.cz/normy-a-pravni-predpisy-facility-management/17479-prava-subjektu-udaju-podle-gdpr-hrozba-pro-provozovatele-kamerovych-systemu-ii-pravo-na-vymaz >.

5. ÚŘAD pro ochranu osobních údajů. *Co dělat, když soused používá kameru*? [online]. uoou.cz, 2. 5. 2018 [cit. 20. března 2020]. Dostupné na < https://www.uoou.cz/co-delat-kdyz-soused-pouziva-kameru/ds-5283/archiv=0&p1=2619>.

6. ÚŘAD pro ochranu osobních údajů. *K provozování kamerových systémů* [online]. uoou.cz, 2. 5. 2018 [cit. 20. března 2020]. Dostupné na < https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099>.

7. RADKOVIČOVÁ, Lucie. *Kamery v bytovém domě a právní povinnosti* [online]. radkovicova.cz, 19. července 2016 [cit. 17. července 2020]. Dostupné na <https://radkovicova.cz/2016/07/kamery-v-bytovem-dome-a-pravni-povinnosti/ >.

8. BUREŠOVÁ, Radana. *Kamerový záznam jako důkaz poškození majetku* [online]. fulsoft.cz, 14. března 2018 [cit. 25. července 2020]. Dostupné na <https://www.fulsoft.cz/33/kamerovy-zaznam-jako-dukaz-poskozeni-majetku-uniqueidmRRWSbk196FNf8-jVUh4EphuCjGAxFFf2R58d4zq4ddrJfTGJxQrnQ/>.

Ostatní zdroje

1. Stanovisko Úřadu č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů

2. Stanovisko Úřadu č. 1/2016: Umístění kamerových systémů v bytových domech, ve znění revize červen 2018

3. Stanovisko č. 4/2004 WP29 ke zpracování osobních údajů prostředky kamerového sledování

4. Guidelines 3/2019 on processing of personal data through video devices

5. Seznam druhů operací zpracování (ne)podléhající požadavku na posouzení vlivu na ochranu osobních údajů. Dostupné na <https://www.uoou.cz/povinnosti-spravcu/ds-5856/archiv=0&p1=3938 >.

Abstrakt

Diplomová práce se zabývá problematikou používání bezpečnostních kamer bytovými domy. Práce obsahuje charakteristiku základních pojmů a vymezení právního rámce.

V dalších částech práce jsou řešeny jednotlivé podmínky pro zavedení a užívání kamerového systému.

Součástí práce jsou také rozhodnutí soudů, které v této oblasti poskytly odpovědi na řadu sporných otázek související s touto problematikou.

Abstract

The diploma thesis deals with the issue of using security cameras by buildings with apartments. The thesis contains the characteristics of basic concepts and the definition of the legal framework.

In other parts of the work, there are solved individual conditions for the installation and using system of camera.

The work also includes decisions of courts, which in this area provided answers to a number of controversial issues related to this issue.

Klíčová slova

osobní údaj, ochrana osobních údajů, GDPR, Úřad pro ochranu osobních údajů, zpracování, správce, provozovatel, kamerový systém, kamerový záznam,

Key words

personal data, personal data protection, GDPR, Office of Personal Data Protection, processing, administrator, system of camera, recording