Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Analýza zákona o zpracování osobních údajů a prolomení hranic ochrany soukromí osob ve veřejném zájmu

Martina Kohoutová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Martina Kohoutová

Hospodářská politika a správa
Veřejná správa a regionální rozvoj

Název práce

Analýza zákona o zpracování osobních údajů a prolomení hranic ochrany soukromí osob ve veřejném zájmu.

Název anglicky

Analysis of the personal data processing law and breaking privacy protection of persons in public interest

---

Cíle práce

Cílem práce je analýza zákona o zpracování osobních údajů, zák. č. 110/2019 Sb.,
zjišťování, jaký je stav na úseku ochrany osobních údajů po přijetí směrnice EU o GDPR, výkon této ochrany a prolomení jejích hranic ve veřejném zájmu. Případně, při zjištění neurčitosti nebo neúplnosti právní úpravy v této oblasti navržení možné úpravy příslušného zákona.

Metodika

-soustředění právních předpisů a odborné literatury ke zkoumanému problému

-konzultace s vedoucím práce

-prostudování právních předpisů a literatury k teoretické části práce a jejich

zhodnocení

-získání a prostudování konkrétních materiálů

-vyhodnocení získaných dat

-sumarizace vyýsledků zkoumání a jejich hodnocení

V Praze dne 23. 06. 2021

Doporučený rozsah práce

60-80 stran

Klíčová slova

Osobní údaj, ochrana osobnosti, fyzická osoba, základní lidská práva, veřejný zájem

---

Doporučené zdroje informací

BARTOŇ, M. a kol. Základní práva. Praha: Leges, 2016. ISBN 978-80-7502-128-1.

ČAPEK, J. Evropský soud a Evropská komise pro lidská práva: Přehled judikatury a nejzávaznějších případů. Praha: Linde, 1995. ISBN 80-85647-64-8.

HAVLÍČEK, A. Lidská a přirozená práva v dějinách. Ústí nad Labem. Universita Jana Evangelisty Purkyně, Fakulta filosofická, 2014. ISBN 978-80-7414-620-6.

MOLEK, P. Základní práva. Svazek první, Důstojnost. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-167-5.

NULÍČEK M. DONÁT J. et al. Zákon o zpracování osobních údajů. Praktický komentář.Wolters Kluver, Praha 2019. ISBN 978-80-7598-467-8

ONDŘEJOVSKÁ, E. Ochrana osobnosti v common low a českém právu. Praha: Leges, 2016. ISBN 978-80-7502-164-9.

PAVLÍČEK, V. a kol. Ústavní právo a státověda. Ústava právo České republiky. Praha: Leges, 2020. ISBN 978-80-7502-468-8.

WAGNEROVÁ, E. a kol. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer, 2012. ISBN 978-80-7357-750-6.

zák.č. 89/2012 Sb., občanský zákoník; zákon č. 110/2019 Sb., zákon o zpracování osobních údajů

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

JUDr. Eva Kadlecová

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 15. 2. 2021

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 15. 2. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 23. 06. 2021

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Analýza zákona o zpracování osobních údajů a prolomení hranic ochrany soukromí osob ve veřejném zájmu" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 29. 11. 2021 _____

Poděkování

Ráda bych touto cestou poděkovala JUDr. Evě Kadlecové, vedoucí diplomové práce, za odbornou pomoc, cenné připomínky, doporučení a odborné vedení v průběhu zpracování této diplomové práce.

Analýza zákona o zpracování osobních údajů a prolomení hranic ochrany soukromí osob ve veřejném zájmu

Abstrakt

Tématem diplomové práce je zpracování osobních údajů a prolomení hranic ochrany soukromí osob ve veřejném zájmu. Cílem této práce je výzkum, zpracování osobních údajů v historickém kontextu i v současné právní úpravě a následné průběžné provedení analýzy této právní úpravy zákona 110/2019 Sb., o zpracování osobních údajů, zjištění stavu na úseku ochrany osobních údajů po přijetí směrnice EU o GDPR, výkon této ochrany. V další části práce je podán výklad o využití kamerových systémů i jiných novodobých trendů v oblasti monitorovacích zařízení a technologií s rozšířením o různé druhy specifické administrativy nutné k provozování těchto systémů v souvislosti s propojením zákona o zpracování osobních údajů, v návaznosti s některými zvláštními oblastmi dění, ale i případného promítnutí do praxe. Dále je práce doplněna o názornou ukázku příkladu z praktického života, o jejím průběhu, který se opírá o problematiku monitoringu zaměstnanců na pracovišti. Závěr práce zahrnuje úvahu o negativech a pozitivech, která s sebou monitoring kamerovými systémy ale i jiná monitorovací zařízení v souvislosti se zákonem 110/2019 Sb., o zpracování osobních údajů přináší.

Klíčová slova: osobní údaj, ochrana osobnosti, fyzická osoba, základní lidská práva, veřejný zájem, ochrana soukromí, drony.

Analysis of the personal data processing law and breaking privacy protection of persons in public interest

Abstract

The topic of this diplomma thesis is processing of personal data and breaching the boundaries of protection of personal privacy in public interest. The main goal of this thesis lies in dealing with the issue of processing personal data in historical context, as well as in current law, in consecutive analysis of the Czech Act n.110/2019, of personal data processing, and also in ascertainment of what state is protection of personal data in, after the reception of EU GDPR directive, and the execution of this protection. In the next part of this thesis, commentary on the usage of camera systems follows, as well as other current trends in the field of monitoring devices and technologies, extended by different types of specific administration required to operate these systems in context of the Czech Act n.110/2019, of personal data processing , in continuity with several special fields of use, as well as potential use in practice. Furthermore, the thesis is supplemented by illustrative example from ordinary life (and its proceeding), which deals with the issue of monitoring employees in workplace. Conclusion of the thesis summarizes reasoning of the negatives and positives, which the use of monitoring camera systems brings (as well as other monitoring devices), in context of the Czech Act n.110/2019, of personal data processing.

Keywords: Personal data, protection of personality, natural person, basic human rights, public interest, privacy protection, drones.

Obsah

Seznam použitých zkratek

Právní předpisy

kompetenční zákon – zákon č. 2/1969, o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky

kontrolní řád – zákon č. 255/2012 Sb., o kontrole (kontrolní řád)

Listina – nebo LZPS Listina základních práv a svobod - usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky

Nařízení – 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)

občanský zákoník – OZ nebo ObčZ., zákon č. 89/2012 Sb., občanský zákoník

ochrana osobních údajů – zákon č. 101/2000 Sb., o ochraně osobních údajů

přestupkový zákon – zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich

s. ř. s. / soudní řád správní – zákon č. 150/2002 Sb., soudní řád správní

SEU – Smlouva o Evropské unii

SFEU – Smlouva o fungování Evropské unie

směrnice 95/46/ES – směrnice Evropského parlamentu a Rady 95/46/ES ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pobytu těchto údajů

trestněprávní směrnice 2016/680 – směrnice Evropského parlamentu a Rady (EU) 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV

správní řád – zákon č. 500/2004 Sb., správní řád

tiskový zákon – zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dílčích zákonů (tiskový zákon)

trestní řád – Tr.Ř., zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

trestní zákoník –Tr.Zák., zákon č. 40/2009 Sb., trestní zákoník

Úmluva – Úmluva o ochraně lidských práv a základních svobod - sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o Úmluvě o ochraně lidských práv a základních svobod

zpracování osobních údajů – zákon č. 110/2019 Sb., o zpracování osobních údajů

Ostatní zkratky

CCTV – kamerový systém se záznamem

ČR – Česká republika

ESLP – Evropský soud pro lidská práva

EU – Evropská unie

MKDS – Městský kamerový dohlížecí systém

NSS – Nejvyšší správní soud

SDEU – Soudní dvůr Evropské unie

SVJ – Společenství vlastníků jednotek

Úřad, ÚOOÚ – Úřad pro ochranu osobních údajů

1. Úvod

Zaměřením této diplomové práce je analýza zákona č. 110/2019 Sb., o zpracování osobních údajů a prolomení hranic ochrany soukromí osob ve veřejném zájmu. Mou volbou se toto téma stalo především proto, že se týká každého z nás. Ochrana osobních údajů je tedy velmi důležitým, složitým a nedoceněným tématem jak pro jednotlivce, tak pro celou společnost.

Pojem osobní údaj zahrnuje identifikační údaje o fyzické osobě, kterými jsou jméno, příjmení, adresa, datum narození, telefonní číslo, obrazový a zvukový záznam, ale i IP adresa počítače nebo jiné lokační údaje. „*Vymezení pojmu osobní údaj je z hlediska problematiky ochrany osobních údajů zásadní, protože jen osobním údajům je v kontextu ZOOÚ a GDPR poskytnuta ochrana. Údaje, které nenaplňují definiční znaky pojmu osobní údaj sice mohou být rovněž chráněny, avšak prostřednictvím jiných právních mechanismů, mezi které se řadí například institut ochrany osobnosti podle občanského zákoníku.*“[1] Osobní údaje nás doprovázejí od kolébky do konce života a nelze si již představit jakoukoli oblast života ve společnosti, kde by nedocházelo ke zpracování osobních údajů alespoň v nějaké podobě. Díky těmto okolnostem se ochraně osobních údajů dostává velké pozornosti jak ze strany odborníků, tak i ze strany široké veřejnosti. V běžném životě, na úřadech, u lékaře nebo při nástupu do nového zaměstnání, všude tam poskytujeme naše osobní údaje. Každým dnem při jakékoli činnosti, kdy jsme na ulici, v obchodech, bankách monitorování kamerovými systémy, jakákoli návštěva internetu či případná platba za použití bankovní karty je monitorována a hodnocena marketingovými společnostmi pro přípravu cílené reklamy a zvýšení případného odbytu zboží, zde všude dochází k podrobnému zpracování osobních údajů, a tedy i k potencionálnímu ohrožení soukromí fyzických osob. Příkladem může být i to, kdy většina z nás hojně využívá sociální sítě, kde, aniž bychom si to vůbec uvědomovali, rádi a dobrovolně o sobě zveřejňujeme celou řadu citlivých soukromých informací, videí a fotografií, které mohou být kýmkoli hravě zneužity proti nám samým, kdy k tomuto zneužití může dojít z kteréhokoli koutu naší planety. Člověk se stále více stává jen číslem v globalizovaném světě, ztrácí svoji

[1] NONNEMANN, František, KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů.* Praha: C. H. Beck, 2012. 50 s. (§ 4 písm. a))

individualitu, originalitu, ale i soukromí, v této době nabývá ochrana soukromí a osobních údajů na stále větším celospolečenském významu. Zajímavý je i pohled na ochranu osobních údajů napříč celou Evropskou unií a její novou legislativou, kterou se snaží o sjednocení a zajištění vyšší ochrany osobních údajů občanů členských států před zneužitím. Evropská unie toto realizuje prostřednictvím obecných nařízení a představuje nový právní rámec ochrany osobních údajů. Toto vše a mnohá další jsou témata, kterými se bude zabývat tato diplomová práce, která se snad stane mnohým prospěšná.

2. Cíl práce a metodika

2.1. Cíl práce

Cílem této práce je zjištění dopadu aplikace právní úpravy zákona č. 110/2019 Sb., o zpracování osobních údajů, na současné zpracovávání osobních údajů v některých oblastech. Přijetím směrnice EU o GDPR mělo dojít k prohloubení ochrany osobních údajů, což bude též předmětem zkoumání. Práce má za cíl komplexně analyzovat právní úpravu, poukázat na její možné nedostatky a navrhnout řešení. Zároveň má pak pojednat a vyhodnotit aplikaci zmíněné právní úpravy v praxi, a to nejen u orgánů veřejné moci, ale především u subjektů (správců), které s osobními údaji občanů pracují, respektive je zpracovávají. Práce bude zejména zaměřena na možnost prolomení hranice ochrany soukromí osob ve veřejném zájmu a na zjištění případných nedostatků v této oblasti.

Speciálně se pak autorka práce hodlá věnovat zkoumání monitoringu osob za využití kamerového systému, výsledkem čehož má být zhodnocení současných trendů při provozu tohoto systému a zjištění legislativních problémů při aplikaci právních norem do praxe, při užití reálných příkladů a úvah de lege ferrenda v tomto směru.

Možným přínosem z této práce je i navržení úpravy či doplnění právních předpisů, a to v případě, že v průběhu práce bude zjištěna neurčitost či neúplnost právní úpravy. Určení nedostatků právní úpravy a navržená opatření k nápravě by pak měly vést ke zvýšení ochrany soukromí, ochrany osobních údajů a dalších aspektů spojených s touto oblastí práva.

2.2. Metodika

Práce bude rozdělena na dvě části – teoretickou a praktickou část. Předkládaná diplomová práce bude zpracována na základě studia odborné literatury přímo související s tématem zpracování osobních údajů a ochrany soukromí osob a platných právních předpisů, zároveň pak i studia rozhodnutí obecných (okresních/krajských) soudů, jež se přímo či nepřímo dotýkají daného tématu, neboť judikatura vzhledem ke krátké době účinnosti zákona

č.110/2019 Sb., o zpracování osobních údajů, nejvyšších soudů se dosud formuje a judikátů je k tomuto tématu poskrovnu. Jedním z mála nalezených vhodných judikátů bude rozhodnutí Nejvyššího správního soudu o kasační stížnosti proti usnesení Městského soudu v Praze a vrácení Městskému soudu k dalšímu projednání, ve věci vyřízení žádosti o přístup k osobním údajům poskytnuté podle § 30 odst. 4 zákona č. 110/2019 Sb., o zpracování osobních údajů, které je rozhodnutím ve smyslu § 65 odst. 1 s. ř. s. a stížnost či podnět k Úřadu pro ochranu osobních údajů směřující proti tomuto rozhodnutí nejsou řádnými opravnými prostředky podle § 5 ve spojení s § 68 písm. a) s. ř. s.

Základní metodou použitou při vypracovávání teoretické části je komplexní analýza právních předpisů týkajících se ochrany osobních údajů a ochrany soukromí stanovených především zákonem č. 110/2019 Sb., o zpracování osobních údajů a další související legislativy. Součástí teoretické části bude taktéž popis historického vývoje ochrany osobních údajů v našem právním řádu. Při teoretické části bude využita metoda evalvace, komparace a popisu při zkoumání jednotlivých ustanovení právních předpisů. Práce bude zpracována na základě prostudování odborné literatury a rešerší přímo související s tématem ochrany osobních údajů s využitím publikací Zákon o zpracování osobních údajů, GDPR Praktická příručka implementace.[2]

Praktická část bude vypracována za použití popisu příkladů z praxe, jejich komparace a evalvace. Na základě dosažených zjištění bude proveden souhrn možných opatření, doplněný úvahami de lege ferrenda, která by ve svém důsledku měla vést k eliminaci zjištěných nedostatků při uvádění legislativních nástrojů do praxe, a tím i zvýšení úrovně ochrany soukromí ve spojitosti se zpracováním osobních údajů.

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

3. Historický vývoj zpracování osobních údajů

Pro představu vývoje ochrany soukromí a zpracování osobních údajů probíhajícího na území České republiky je nutné alespoň částečně nahlédnout do historie. Před vznikem samostatné Československé republiky byla naše země součástí Rakouského císařství. Dne 1. června 1811 byl vyhlášen Všeobecný zákoník občanský, a sice patentem císaře Františka I., který zůstal v platnosti až do roku 1951, kdy byl nahrazen československým občanským zákoníkem č. 141/1950. Tento Všeobecný zákoník občanský se původně jmenoval Allgemeines bürgerliches gesetzbuch (zkr. „ABGB“) a po vzniku republiky v roce 1918 byl přijat tzv. recepční normou – zákonem č. 11/1918, který přejímal, ponechával v platnosti a účinnosti dosud fungující zákony z Rakouského císařství, dokud nebyly nahrazeny vlastními, československými předpisy. Po vzniku samostatného československého státu v roce 1918 byla přijata takzvaná **Prozatímní ústava** zákon č. 37/1918 Sb., o prozatímní ústavě, na ni následně navazovala **Ústavní listina Československé republiky**, která byla vyhlášena pod č. 121/1920 Sb., a obsahovala souhrn základních lidských občanských práv, svobod a povinností. Tato ústava byla doplněna **ústavním zákonem** č. 293/1920 Sb., **o ochraně svobody osobní, domovní a tajemství listovního a zákon** č. 300/1920 Sb., **o mimořádných opatřeních**, účinností od 6. 5. 2020 zakládal vládě republiky pravomoc vydat nařízení o mimořádném opatření, podléhající schválení prezidentem republiky. V tomto zákonu byly upraveny okolnosti a důvody, za kterých bylo možno dočasně omezit či rušit svobody založené Ústavní listinou – svobodou osobní § 107, domovní § 112, tiskovou § 113 a právo shromažďovací a spolkové, listovní tajemství § 116 a svobody konkrétně rozepsané v Ústavním zákoně č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního. Tento Ústavní zákon konkretizoval výše uvedené svobody a umožnil jejich prolomení v rámci např. trestního řízení. Tohoto omezení bylo ve skutečnosti využito, např. Nařízením vlády republiky Československé 636/1920 Sb., ze dne 12. 12. 1920. Základními právy osob se zabývala především Ústava ČR, ale v české právní praxi existoval ještě již výše zmíněný **Všeobecný zákoník občanský,** který byl základním kamenem občanského práva.

*„Později následovalo **temné období**, kterým byla **okupace** tehdejšího Československa a vznik Protektorátu Čechy a Morava (č. 75/1939 Sb.), protiprávní akt, kterým byly likvidovány všechny existující svobody českého národa. Přestala být uznávána zásada*

rovnosti před zákonem, protože právo bylo aplikováno různě podle třídní, rasové a politické příslušnosti obžalovaného.“[3]

Na toto nechvalně proslulé období navázalo **dlouhé období totality**, ve kterém se řešila pouze pravidla ochrany osobních údajů v souvislosti s vydáváním a držením cestovních dokladů nebo jiných dokladů. Ochrana osobních údajů nebyla nijak regulována, neboť by to neodpovídalo zájmům totalitního státu, kdy byla orgány veřejné moci často vedena složka na jednotlivé občany. Osobní údaje fyzických osob byly zpracovávány bez validace zákonem, k prolomení „ochrany“ v tehdejším pojetí docházelo zvůlí příslušníků Státní bezpečnosti, aniž by bylo s osobou mnohdy zahájeno trestní řízení, nebo aniž by zde existoval jiný právní důvod vyjma údajné prevence „rozvracení státu“.

Změna nastala až s přijetím **Listiny základních práv a svobod** usnesením předsednictva České národní rady č. 2/1993 Sb., ze dne 16 prosince 1992 jako součásti ústavního pořádku České republiky.

Ochrana osobních údajů v České republice je na ústavní i zákonné úrovni. V oblasti ochrany osobních údajů byl prvním komplexním právním předpisem zákon č. 256/1992 Sb. o ochraně osobních údajů v informačních systémech. Tento zákon reagoval na Úmluvu č. 108, kterou v roce 1981 přijala Rada Evropy. Přínosným se tento zákon stal především tím, že uvedl definice základních pojmů, jako například provozovatel informačního systému, informační systém nebo **osobní údaj**. Jako nedostatečný byl vnímán fakt, že nevznikl žádný orgán kontroly, který by zajistil dohled nad nakládáním s osobními údaji. Nedostatkem byla i absence sankcí jako důsledku porušení pravidel ochrany dat stanovených v zákoně.

V oblasti ústavního pořádku je právo na ochranu osobních údajů zabezpečeno Listinou základních práv a svobod. **Listina základních práv a svobod** (dále LZPS nebo Listina), byla přijata Ústavním zákonem č. 2/1993 Sb., následně ve znění Ústavního zákona č. 162/1998 Sb., obsahuje základní lidská práva a svobody, politická, hospodářská, kulturní, sociální práva, ale i právo národnostních, etnických menšin, dále i právo na soudní a jinou právní ochranu.

---

[3] VOJÁČEK, Ladislav, SCHELLE, Karel. *České právní dějiny do roku 1945.* 1. vydání. Ostrava: KEY Publisching, 2007. 218 s. ISBN 987-80-87071-20-5. str. 206.

Článek 1 pojednává o lidské rovnosti, důstojnosti a právech, o nezadatelnosti, nezcizitelnosti, nepromlčitelnosti těchto základních lidských práv a jejich nesporné důležitosti a významu pro každého jedince. Není možné, aby byla tato základní lidská práva komukoli upírána, omezena či odňata. V platnosti je i skutečnost, kdy v případě trvalé vymahatelnosti je možné domoci se svých práv později a práva jednotlivce není možné státem zrušit, případně prohlásit za neplatná. Tato práva nelze ani převést na kohokoli jiného.

Článek 2 pojednává o demokratických hodnotách, na kterých je náš stát založen a o řádném uplatnění zákona. Zaveden je též ústavní princip legální licence, který znamená, že co není zakázáno, je dovoleno - hranice jsou jen v mezích zákona, svoboda je ohraničena svobodami druhých. Naopak státní moc ale lze uplatňovat pouze v případech a v mezích zákona, a to způsobem, který stanoví zákon *(secundum et intra legem).*

Článek 3 se v odstavci 1 zaměřuje na základní práva a svobody bez rozdílu pohlaví, rasy, barvy pleti, jazyka, víry a náboženství, politického či jiného smýšlení, národního nebo sociálního původu, příslušnosti k národnostní nebo etnické menšině, majetku, rodu nebo jiného postavení.

Článek 4 uvádí povinnosti spojené s ukládáním zákona, kdy připouští zásah do lidských práv jednotlivce jen na základě zákona a pouze v nezbytně nutné míře, za předpokladu zachování práv a svobod jednotlivce.

Článek 7 se zabývá nedotknutelností jedince a jeho soukromí.

Článek 10 v prvním odstavci je z pohledu ochrany osobnosti velmi významný především proto, že je zde zdůrazněno právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a ochrany jeho jména.

Ve druhém odstavci tohoto článku je též zakotveno právo na ochranu před neoprávněným zásahem do soukromého a rodinného života.

V následujícím třetím odstavci dále i právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Článek 12 zaručuje nedotknutelnost obydlí a specifikuje, za jakých podmínek je umožněn zásah do nedotknutelnosti obydlí – dle zákona.

Článek 13 zde je uvedeno, že se nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, kdy smyslem je garance ochrany dopravovaných zpráv, týkající se i elektronických sdělení a SMS. Je ale nutné si uvědomit, že každá z těchto zásad má **výjimky**, které ovšem také vycházejí ze zákona, ať už se jedná např. o trestní zákoník či zákon o odpovědnosti za přestupky.

Listina základních práv a svobod vytváří v České republice základní pilíř pro uplatnění práva na ochranu osobních údajů. Základní ustanovení jsou rozšířena o právní předpisy nižší právní síly. Zde se spíše jedná o ústavní zásady, které jsou kodifikovány na úrovni běžných zákonů.

Právní předpis, kterým došlo v České republice ke sjednocení ochrany osobních údajů s dalšími státy Evropy, je zákon č. 101/2000 Sb., ze dne 4. 4. 2000, o ochraně osobních údajů a o změně některých zákonů, tento zákon nabyl účinnosti 1. 6. 2000.

Jednalo se o důležitý obecný první právní předpis, ve kterém došlo ke komplexní úpravě a nahrazení předchozího zákona č. 256/1992 Sb.; o ochraně osobních údajů v informačních systémech.

Následně byl v souvislosti s tímto zákonem zřízen i dosud chybějící **„Úřad pro ochranu osobních údajů“** (dále jen ÚOOÚ), tento Úřad je jediným dozorovým úřadem s obecnou působností podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES v České republice.

Samotný ÚOOÚ specifikuje svou působnost v rámcích zákona takto:

„Posláním Úřadu je napravit chybné procedury zpracování osobních údajů správci nebo zpracovateli osobních údajů. Nezabývá se proto každým porušením ochrany soukromí; je věcí poškozeného, aby se domohl nápravy žalobou u soudu. Úřad se zabývá nedostatečnou ochranou osobních údajů, která má systémový přesah, tj. z její nápravy bude profitovat větší množství subjektů údajů.

Kromě ochrany osobních údajů plní Úřad další úkoly svěřené mu zákonem. Jedná se o tyto oblasti:

- ***elektronické identifikátory** podle § 11 zákona č. 111/2009 Sb., o základních registrech,*
- ***svobodný přístup k informacím** podle § 16b zákona č. 106/1999 Sb., o svobodném přístupu k informacím,*
- ***elektronické komunikace** podle § 87 odst. 4 zákona č. 127/2005 Sb., o elektronických komunikacích,*
- ***šíření obchodních sdělení** podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti),*
- ***zvláštní dozor**, například § 80b odst. 3 věta druhá a § 80c odst. 4 věta první zákona č. 273/2008 Sb., o Policii České republiky, a*
- ***zvláštní správní trestání**, například §§ 16a–16c zákona č. 328/1999 Sb., o občanských průkazech, § 34a odst. 4 a § 34c odst. 4 zákona č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o cestovních dokladech), § 17e odst. 6 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel) a § 25 odst. 2 zákona č. 159/2006 Sb., o střetu zájmů.“*[4]

Úřad dohlíží na ochranu soukromí a osobních údajů. V rámci dozorové činnosti, Úřad vykonává kontrolní činnost podle kontrolního řádu zákon č. 255/2012 Sb., zákon o kontrole (kontrolní řád) a plní řadu úkolů, které sledují zkvalitnění a prohloubení ochrany osobních údajů v Evropském hospodářském prostoru i v případě jednotlivých správců. Zákon o ochraně osobních údajů byl po dobu své účinnosti průběžně novelizován, jedna z novel proběhla v souvislosti se vstupem České republiky do Evropské unie v roce 2004 a nutností zavedení legislativy Evropské unie prostřednictvím směrnice 95/46/ES do českého právního řádu, která představuje normu v oblasti ochrany osobních údajů na evropské

[4] Úřad pro kontrolu osobních údajů. Dostupné z [online]: https://www.uoou.cz/pusobnost/ds-1269/archiv=0&p1=1059.

úrovni. Cílem je zavedení jednotného právního rámce mezi ochranou osobních údajů a volným pohybem osobních údajů po Evropské unii. Tato Evropská legislativa se váže k údajům, které jsou zpracované automaticky, jakými jsou např. počítačové databáze, neautomatizované údaje, tedy ty údaje, které jsou vedeny v tradiční listinné podobě. Evropská legislativa si v tomto případě klade za cíl ochranu práv a svobod osob v návaznosti na zpracování osobních údajů. Tyto osobní údaje musí být **zpracovány přesně, bezchybně** na základě zákona a **uchovávány mohou být pouze po dobu nezbytně nutnou** ke splnění účelu, pro který jsou shromážděny.

Od 25. května 2018 v České republice vešlo v platnost **Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES** (dále jen „Obecné nařízení“ nebo „GDPR“), které v českém právním řádu lze uplatnit v plném rozsahu, zároveň dává možnost všem členským státům EU upřesnit nebo rozšířit ustanovení v tomto nařízení uvedená. Díky tomuto byl v České republice přijat **zákon č. 110/2019 Sb., o zpracování osobních údajů,** kterým byl zrušen stávající zákon o ochraně osobních údajů, **zákon č. 101/2000 Sb., o ochraně osobních údajů a některých navazujících zákonů.**

4. Rozbor právní úpravy

4.1. Základní informace o zákonu č. 110/2019 Sb., o zpracování osobních údajů

Na jaře 2016 bylo přijato **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.** Od 25. května 2018 po uplynutí dvouletého přechodného období vstoupilo toto nařízení v platnost a nahradilo směrnici 95/46/ES. **GDPR také nahradilo vnitrostátní právní předpis**y implementující směrnici 95/46/ES ve všech členských státech Evropské unie a tedy i v České republice. Od tohoto data je právem a povinností správců, zpracovatelů i subjektů osobních údajů vycházet přímo z tohoto Obecného nařízení. Platnost zákona č. 101/2000 Sb. o ochraně osobních údajů byla ukončena až po jeho zrušení adaptačním předpisem, tento zákon do té doby dočasně upravoval působnost a výkon pravomocí Úřadu pro ochranu osobních údajů. Dne 25. května 2018 nahradilo Obecné nařízení zákon č. 101/2000 Sb., o ochraně osobních údajů. Nařízení je přímo aplikovatelné v českém právním řádu, zároveň ale umožňuje členským státům upřesnit nebo rozvést ustanovení, která jsou v něm zakotvená. Z tohoto důvodu byl u nás přijat nový zákon č. 110/2019 Sb., o zpracování osobních údajů.

„Zákon o zpracování osobních údajů nabyl účinnosti 24. 4. 2019, nicméně adaptační legislativa k Nařízení měla být přijata do 25. 5. 2018 a transpoziční legislativa ke směrnici 2016/680 měla být přijata do 6. 5. 2018. V mezidobí se tak stihla vyrojit celá řada spekulací, např. že se požadavky Nařízení bez zákona o zpracování osobních údajů neuplatní, že režim dle Nařízení není bez zákona o zpracování osobních údajů kompletní, popřípadě že zákon o zpracování osobních údajů přinese oproti režimu dle Nařízení zásadní zmírnění pro všechny správce a zpracovatele. Nic z toho se nezakládá na pravdě – Nařízení bylo v plném rozsahu účinné a aplikovatelné již od 25. 5. 2018.“[5]

Společně s **adaptačním zákonem č. 110/2019 Sb.,** nabyl účinnosti zákon č. 111/2019 Sb., kterým se mění některé zákony spolu s přijetím zákona o zpracování osobních údajů.

---

[5] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. XIII.

4.2. Analýza zákona č. 110/2019 Sb., o zpracování osobních údajů

4.2.1. Část první – Zpracování osobních údajů

Zákon č. 110/2019 Sb., o zpracování osobních údajů, který upravuje pro české prostředí nařízení Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (GDPR) a transponuje směrnici 2016/680 (dále jen „nařízení GDPR“, nebo „GDPR“) **. Jak autorka již uvedla výše, jedná se o komplexní zákon,** je to norma veřejnoprávní, norma kogentní, norma hmotněprávní. Většina veřejnoprávních norem jsou skutečně kogentní, ale ne vždy tomu tak je. **Kogentní normu** však odvozujeme přímo od jejího obsahu, nikoliv zařazení do právního systému. Pokud norma převážně zakazuje nebo říká, že někdo „musí, nesmí, je povinen, nesmí se od normy odchýlit“, tak ji považujeme za kogentní. Naopak dispozice – „může, smí, je možno dojednat nad rámec normy“, to zakládá normu dispozitivní. Existují i kombinované normy – např. zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů. Zaměstnavatel je povinen řídit se určitými pravidly, ale zároveň se mu dovolují věci nad rámec zákona, pokud budou ve prospěch zaměstnanců.

4.2.1.1. Hlava I – Základní ustanovení

Hlava I, vymezuje předmět právní úpravy, působnost zákona o zpracování osobních údajů a subjekt údajů, tedy fyzickou osobu, ke které tyto osobní údaje náleží.

Prvním z mnoha důležitých pojmů je **osobní údaj**, který je Janečkovou ve zkratce vymezen jako *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě – o subjektu údajů.“*[6] Je zásadní na tomto místě podotknout, že náš zákon se nezabývá definicí **osobního údaje**, neboť tento je již specifikován v čl. 4 odst. 1 nařízení GDPR, takto: *„osobními údaji“ se rozumí 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 na jeden či*

[6] JANEČKOVÁ, Eva. GDPR. Praktická příručka implementace. Praha: Wolters Kluwer ČR, 2018. 136 s. ISBN 978-80-7552-248-1. str. XI

více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;"[7]

V **§ 1** jsou podrobně začleněny jednotlivé předpisy Evropské unie, které vytváří přímou kontinuitu na předpis Evropské unie k možnému právnímu uplatnění jednotlivce na ochranu soukromí, zároveň provádí úpravu práv a povinností pro zpracování osobních údajů.

V tomto paragrafu je uveden pojem **zpracování osobních údajů,** který je podle nařízení definován jako *„jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení."*[8] Zpracování osobních údajů nezahrnuje pouhé nakládání s osobními údaji, zde se jedná o velmi sofistikovanou činnost, kterou správce provádí metodickým a plánovitým přístupem. Pojem zpracování má dle GDPR stejný význam jako v zákonu č. 101/2000 Sb., o ochraně osobních údajů.

Zpracování osobních údajů je považováno za postup nebo systém postupů, které se systematicky provádějí při nakládání s osobními údaji a ochrana osobních údajů je součástí ochrany soukromí jako jednoho ze základních lidských práv.

V následujícím **§ 2** je upravena působnost zákona ochrany osobních údajů ve **třech oblastech:**

První oblast se zabývá zpracováním osobních údajů podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Veškeré činnosti spadající do působnosti práva EU, výjimku tvoří prevence a potírání kriminality, předcházení bezpečnostním hrozbám, obrana a národní bezpečnost.

---

[7] https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679#d1e1396-1-1

[8] JANEČKOVÁ, Eva. GDPR. Praktická příručka implementace. Praha: Wolters Kluwer ČR, 2018. 136 s. ISBN 978-80-7552-248-1. str. XII

Druhou je činnost všech orgánů činných v trestním řízení, policejního zaměření s orientací na prevenci kriminality, předcházení bezpečnostním hrozbám nebo dalších orgánů, které mohou být v přímém kontextu s trestním řízením.
Třetí je oblast národní bezpečnosti, zajištění veřejného pořádku a vnitřní bezpečnosti.
Dále pak zabezpečování ochranných a bezpečnostních zájmů při zpracování osobních údajů, stejně tak jako zpracování osobních údajů určených pro evidenci a její úplné nebo částečné automatizované zpracování.
Úřad pro ochranu osobních údajů je nezávislým orgánem, který dohlíží na to, aby nedocházelo k porušování předpisů týkajících se osobních údajů, a tím i k zásahům do základních lidských práv a svobod, při zjištění nedostatků ukládá sankce. Další jeho relativně novou pravomocí je možnost přezkumu zákonného postupu povinných subjektů při vyřizování žádostí o poskytnutí informací podle zákona 106/1999 Sb., o svobodném přístupu k informacím. Přezkumná pravomoc Úřadu pro ochranu osobních údajů znamená, že neuspokojení žadatelé o poskytnutí informací získali další prostředek obrany proti pravomocnému rozhodnutí o odmítnutí žádosti o poskytnutí informací. Konkrétně se zákonem zabývá Úřadem v hlavě V, viz níže.

Následující § 3 je jedním z nejpodstatnějších ustanovení, neboť se především zabývá pojmem **subjekt údajů**. Podle definice to je *„identifikovaná fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, např. jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“*[9] Zde je velmi důležité poznamenat, že subjektem údajů jsou pouze žijící osoby. Což znamená, že u osob, které již nejsou naživu a osobní údaje o nich stále existují, měly by být patřičně označeny nebo zlikvidovány.
Zákonodárce zde byl nucen zvolit opačný postup, než tomu bylo u definice **osobního údaje**, jelikož GDPR nedefinuje **subjekt údajů**. GDPR používá termín „subjekt údajů“ ve vztahu k informacím o identifikované nebo identifikovatelné fyzické osobě jako legislativní zkratku. *„Z toho důvodu český zákonodárce pro úplnost vymezuje pojem*

[9] JANEČKOVÁ, Eva. GDPR. Praktická příručka implementace. Praha: Wolters Kluwer ČR, 2018. 136 s. ISBN 978-80-7552-248-1. str. XI.

subjekt údajů, a to stejně jako za předchozí právní úpravy, tedy tak, jak byl pojem subjekt údajů chápán i ve smyslu původního zákona o ochraně osobních údajů.“[10]

Vlachová s Maisnerem vysvětlují, že ve vztahu k právnickým osobám nelze hovořit o ochraně osobních údajů. Na ochranu práv těchto uměle vytvořených subjektů nelze aplikovat zákon o ochraně osobních údajů, nýbrž zákon č. 89/2012 Sb., občanský zákoník, jako obecný předpis. „*Osobními údaji jsou však údaje o lidech, kteří působí v orgánech právnických osob. Úprava v GDPR se vztahuje i na* ***fyzické osoby podnikající.“***[11]

4.2.1.2. Hlava II – Zpracování osobních údajů podle přímo použitelného předpisu Evropské unie

Díl 1

Hlava II, vymezuje působnost ustanovení a rozsah oprávnění zpracování osobních údajů podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46 ES (obecné nařízení o ochraně osobních údajů), které podle **§ 4** mají být nebo které jsou zařazeny do evidence. Uvádí **výčet výjimek** z povinností podle tohoto nařízení a to zejména pokud zpracování osobních údajů vychází z právní povinnosti při plnění úkolů ve veřejném zájmu, zpracování osobních údajů orgány veřejné moci a veřejnými subjekty a etc.

§ 5 zahrnuje oprávnění ke zpracování osobních údajů, tj. vyjasnění, kdy správce má oprávnění ke zpracování osobní údajů nezbytných pro splnění povinností nebo úkolů prováděných ve veřejném zájmu.

„*Veřejný zájem je neurčitý právní pojem, který zůstává i přes hojný výskyt v různých legislativních aktech bez legální definice. Veřejný zájem představuje jakousi snahu o udržování a ochranu celospolečensky významných hodnot.“*[12]

---

[10] VLACHOVÁ, Barbora, MAISNER, Martin. Zákon o zpracování osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2019, 168 s. ISBN 978-80-7400-760-6 s. 7.)
[11] Tamtéž, s. 7
[12] Tamtéž, s. 11.)

Následně v **§ 6** jsou uvedeny výjimky z povinnosti posuzování slučitelnosti účelů

Obsahem prvního odstavce je cílené ulehčení činnosti správcům v případě zpracování nových osobních údajů nezbytných pro plnění povinností pro výkon úkolu ve veřejném zájmu. V případě, že správce zpracovává nezbytné osobní údaje při plnění úkolu ve veřejném zájmu, nemusí se dodržet slučitelnost účelu, pro který byly původně shromážděny.

Správce je podle zákona o ochraně osobních údajů *„každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.“*[13]

Jak uvádí JUDr. Janečková podle Nařízení je **správcem osobních údajů** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jiným určuje účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dodatečného správce nebo zvláštní kritéria pro jeho určení.[14]

Ve druhém odstavci je specifikován pojem **chráněný zájem,** pod který lze zahrnout zajištění bezpečnostních nebo obranných zájmů České republiky, finančních a hospodářských zájmů, ochranu nestrannosti justice, zajištění veřejného pořádku, odhalování protiprávního jednání či ochranu a obhajobu práv a povinností jednotlivce.

„Bezpečnost státu a bezpečnost občanů je také nezbytným předpokladem, aby občané mohli užívat na území státu svých práv a svobod.“[15] Pavlíček dále dělí bezpečnost státu na vnitřní a vnější, přičemž obě složky jsou považovány za zásadní pro uplatňování zmíněných práv a svobod. *„Bezpečnost státu zajišťují především jeho ozbrojené sbory (armáda, policie a další bezpečnostní složky). Povinnosti jsou však státem uloženy i dalším orgánům, organizacím a občanům.“*[16]

---

[13] JANEČKOVÁ, Eva. GDPR. Praktická příručka implementace. Praha: Wolters Kluwer ČR, 2018. 136 s. ISBN 978-80-7552-248-1. str. XI.
[14] JANEČKOVÁ, Eva. GDPR. Praktická příručka implementace. Praha: Wolters Kluwer ČR, 2018. 136 s. ISBN 978-80-7552-248-1. str. XI.
[15] PAVLÍČEK, V. a kol. *Ústavní právo a státověda, II. Díl. Ústavní právo České republiky.* 3 vydání. Praha: Leges, 2020, 1160s., ISBN 978-80-7502-468-8, s. 1059.
[16] Tamtéž, s. 1060

Obzvláště důležitým ustanovením pak je § 6 odst. 2 písm. b), podle kterého se chráněným zájmem rozumí: „*veřejný pořádek a vnitřní bezpečnost,* ***předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkon trestů a ochranných opatření, zajišťování bezpečnosti České republiky*** *nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech.*“

Následující **§ 7** stanovuje, kdy je **dítě způsobilé pro souhlas** se zpracováním osobních údajů. K udělení souhlasu se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti je dítě způsobilé **po dovršení patnáctého roku věku.** Před dosažením věku patnácti let musí být souhlas vyjádřen zákonným zástupcem dítěte, nutné je i hodnověrné ověření, že byl tento souhlas za strany zákonného zástupce udělen.

Předmětem **§ 8** je **informační povinnost**, která je pro případ zpracování osobních údajů upravená zákonem. Toto ustanovení opravňuje správce, kteří při plnění právní povinnosti, popřípadě úkolu ve veřejném zájmu či výkonu veřejné moci, zpracovávají osobní údaje, zveřejňují informace a plní tím tak svoji informační povinnost spojenou se zveřejněním informací umožňující dálkový přístup, které je možné využívat prostřednictvím internetu.

Následující **§ 9** upravuje informační povinnost oznámení formou výchozí evidence, kdy správce je povinen příjemci oznámit provedenou opravu, zpracování, omezení nebo výmaz osobních údajů, a to v případě, že příjemci pravidelně zpřístupňuje obsah vedený v evidenci. Cílem je tedy omezit informační povinnost správců vůči příjemcům v případě změn, výmazů zpracovávaných údajů v evidenci.

V **§ 10** je uvedena **výjimka z povinnosti správce** posouzení vlivu před zahájením zpracování osobních údajů na ochranu osobních údajů. Je nutné, aby správce pokud má povinnost zpracovávat osobní údaje, posuzoval vliv na ochranu a zpracování osobních údajů. Správce je tedy povinen posoudit rizikovost zpracování osobních údajů, především to, zda je či není možné tato rizika minimalizovat.

K **§ 11** se váže možnost **omezení práv a povinností** článek 5 EU obecné nařízení o ochraně osobních údajů, v rámci zajištění úkolů ve veřejném zájmu a oznamovací povinnost správce Úřadu pro ochranu osobních údajů na přijatá opatření v oblasti chráněného zájmu.

V **§ 12** je zahrnuta výjimka k povinnosti oznámit porušení zabezpečení osobních údajů subjektu údajů a **§ 13** zahrnuje osobní údaje s omezeným zpracováním, a to především kdy a za jakých okolností musí správce nebo zpracovatel předat nebo zpřístupnit údaje, u kterých je zpracování omezeno.

Dále v **§ 14** je stanoveno kdy nebo v jakém případě nastává povinnost **jmenovat pověřence** pro ochranu osobních údajů.

Pověřencem může být jak zaměstnanec, tak třetí osoba. U pověřence jako zaměstnance nesmí docházet ke střetu zájmů, proto není možné, aby zastávat pozici, kde by sám zpracovával osobní údaje.

Hlavním úkolem pověřence je *„monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z nařízení, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany dat.“*[17] Celkově shrnuto, hlavní úkol pověřence je sledování dodržování Nařízení a předpisů, mezi které patří:

a.) shromažďovat pouze takové informace, které slouží k identifikaci zpracovatelských činností

b.) provádět analýzu a průběžnou kontrolu shodujících se zpracovatelských činností

c.) poskytovat relevantní informace, rady a vydávat příslušná doporučení správcům, zpracovatelům či pracovníkům ve vedení

Působnost a organizační strukturu v případě akreditace subjektů pro vydání osvědčení o ochraně osobních údajů je definována v **§ 15**.

§ 16 je rozdělen do tří odstavců a souvisí se zpracováním zvláštní kategorie osobních údajů pro účely historického a vědeckého výzkumu nebo statistických účelů, kdy správce by měl chránit, ale i reagovat na případná rizika újmy na právech a svobodách. Zároveň by měl reagovat na případné požadavky a nařízení umožňující zpracovávat citlivé údaje i případnou anonymitu údajů subjektu.

[17] JANEČKOVÁ, Eva. GDPR. Praktická příručka implementace. Praha: Wolters Kluwer ČR, 2018. 136 s. ISBN 978-80-7552-248-1. str. 82.

Díl 2

V druhém dílu je upraveno zpracování osobních údajů prováděné pro novinářské, akademické, umělecké a literární účely.

Následný **§ 17** zapracovává výjimky z práv a povinností na ochranu osobních údajů dle naplnění článku 85 EU obecné nařízení o ochraně osobních údajů, požadující po členských státech uvedení v soulad **s právem na svobodu projevu a informací pro novinářské a obdobné účely**. Informace jsou vyhledávány, tříděny, shromažďovány a zveřejňovány široké veřejnosti, kterými jsou diváci, posluchači, studenti nebo čtenáři k podpoře veřejné diskuze. Toto ustanovení je odezvou práva na informace a je tedy provázáno s článkem 17 odstavec 3 Listiny základních práv a svobod, ve kterém se jedná o zákaz předběžné kontroly zpracování prostřednictvím schvalování nebo povolování Úřadu pro ochranu osobních údajů.

„Lze shrnout, že komentované ustanovení využívá rámec daného Nařízením a legislativně upravuje požadavky na provedení testu proporcionality mezi jednotlivými základními právy. Ochrana osobních údajů jako součást základního lidského práva na soukromí a lidskou důstojnost není neomezitelná a je nutné ji upravit a vykládat tak, aby nedocházelo k nepřiměřenému zásahu do dalších lidských práv.“ [18]

První odstavec **§ 18**, který pojednává o možnosti splnit informační povinnost uvedením identity správce, a to například pomocí grafického označení v podobě visačky, loga nebo ústním prohlášením v situaci, kdy jsou poučeni o právech a informace o standardním zpracování správcem dostupných na jeho internetových stránkách. Další odstavec řeší především, kdy a ve kterých případech je správce oprávněn informaci neposkytovat.

V **§ 19** jsou zakotveny výjimky ochrany zdroje a obsahu informací před možností narušení. Odstavec 1 zavádí informační povinnost správce uvedením požadovaných informací podle článku 14 a 21 EU obecné nařízení o ochraně osobních údajů, zároveň řeší zveřejnění dálkovým přístupem, především šíří subjektů údajů, které jsou cílem těchto informací, kdy je zákonodárcem povoleno informování o obvyklém rozsahu zpracování osobních údajů. V

[18] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 53.

odstavci 2 je v průběhu zpracování osobních údajů (tj. před jejich zveřejněním) omezeno právo na přístup podle článku 15 EU obecné nařízení o ochraně osobních údajů. Ze strany správce je možné omezení práva na přístup, pokud by výkon tohoto práva subjektu ohrozil účel zpracování nebo pokud by neúměrně zatížil správce.

Výjimku z práv na výmaz, opravu a omezení zpracování osobních údajů, je uplatněn v **§ 20** který využívá této možnosti podle článku 85 EU obecné nařízení o ochraně osobních údajů.

§ 22 v tomto paragrafu jsou uvedena omezení práva na námitku, tím je chráněna svoboda tisku i případné ochromení novinářské práce. Námitku lze uplatnit pouze proti konkrétnímu zpřístupnění nebo zveřejnění osobních údajů. Pokud je správce přesvědčen, že případné zájmy subjektu údajů na ochraně práv a svobod nemají převahu nad zájmem na zpracování osobních údajů, nemusí námitce vyhovět.

V **§ 23** se uvádějí další výjimky pro zvláštní případy svobody tisku (médií), ochrana a případná omezení pravomocí dozorového úřadu. V tomto paragrafu jsou stanoveny podmínky, kdy je možné dojít k přiměřenému užití nebo nepoužití výjimek podle § 18 až 22 nebo k částečnému užití nebo neužití článku 12 až 19, 21, 33, 34 EU obecné nařízení o ochraně osobních údajů. V případě článku 21 EU obecné nařízení o ochraně osobních údajů, je zakotveno právo subjektu údajů na vznesení námitky článku 33 a 34 EU obecné nařízení o ochraně osobních údajů, kterým je řešeno ohlašování případů porušení a zabezpečení osobních údajů Úřadu pro ochranu osobních údajů. Mimo přiměřeného užití nebo neužití uvedených ustanovení může dojít k odložení povinností zpracovatele, správce nebo k případnému uplatnění práva subjektu údajů. Dále jsou řešena případná snížení rizika pro oprávněné zájmy subjektu údajů.

4.2.1.3. Hlava III – Ochrana osobních údajů při jejich zpracování za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti.

Hlava III, upravuje pravidla pro ochranu osobních údajů při zpracování osobních údajů navazující na činnost orgánů činných v trestním řízení na základě zákona č. 52/2009 Sb., tento zákon rozšířil znění trestního řádu v oblasti poskytování informací o trestním řízení a osobách na něm zúčastněných, mění se jím zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony. Tato ustanovení provádějí z převážné většiny směrnice 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. Ustanovení se vztahují na některé bezpečnostní sbory a další orgány, které jsou zákonodárcem soustředěny do společného právního předpisu.
§ 24 v obecném ustanovení je upravena především věcná a personální působnost, jsou zde definovány orgány, které se zabývají specifickým plněním úkolů a výkonem veřejné moci v oblasti potírání a prevence trestné činnosti.

Veřejnou mocí se rozumí *„schopnost autoritativně rozhodovat o právech a povinnostech jednotlivců bez ohledu na jejich vůli. Výkon veřejné moci provádějí orgány, které touto mocí disponují, a to vždy na základě a v mezích zákona.“* [19] Vztahuje se pouze na ty orgány, které mají působnost v oblasti prevence a potírání trestné činnosti, při výkonu této působnosti. V odstavci 3 je zákonodárcem uvedeno, že toto ustanovení nedopadá na zpravodajskou službu či obecní policii. **Obecní policie** je podle **zákona č. 553/1991 Sb., o obecní policii** orgánem obce, kdy tento zákon jen rámcově zasahuje do oblasti potírání kriminality a udržování bezpečnosti a není tedy možné jeho srovnání s činností orgánů činných v trestním řízení. V případě zpravodajských služeb se vylučují činnosti agentur či útvarů, které se zabývají národní bezpečností. V následujícím odstavci ustanovením této

[19] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 75.

hlavy podléhá jen takové zpracování osobních údajů, které mají být nebo jsou zařazeny do evidence, nebo pokud toto zpracování probíhá zcela nebo zčásti automatizovaně.

§ 25 V rámci zásad zpracování osobních údajů je definován pojem **spravující orgán,** „ *je povinen při zpracování osobních údajů stanovit konkrétní účel zpracování, který je vyjádřen v § 24 odstavci 1. Osobní údaje tedy mají být shromažďovány pro výslovně vyjádřené a legitimní účely v oblasti potírání a prevence trestné činnosti, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.“*[20] Spravující orgán by měl vždy vyhodnocovat nezbytnost uchování osobních údajů, umožňujících identifikaci subjektu údajů, vzhledem k účelu zpracování. Příkladem může být **Policie České republiky**, kde je podle **§ 82 zákona 273/2008 Sb., o Policii České republiky** obecná lhůta 3 roky. Spravující orgán, který zpracovává osobní údaje, nesouvisející s vyšetřováním a potíráním trestné činnosti, je oprávněn pouze zvláštním zákonem a tento jiný účel nesmí být neslučitelný se stanoveným konkrétním účelem jejich zpracování.

§ 26 je reakcí na směrnici Evropského parlamentu a Rady (EU) 2016/680, požadující rozlišení mezi rozdílnými kategoriemi subjektu údajů, příkladem mohou být osoby, u kterých je možný předpoklad, že došlo ke spáchání trestného činu, u obětí trestných činů, u osob odsouzených za trestný čin, či případných svědků. Zároveň je nutné udržovat osobní údaje aktuální a přesné ve spojitosti s účelem zpracování.

„Ustanovení § 26 ukládá spravujícímu orgánu povinnost evidovat u subjektů údajů jejich procesní postavení v trestním řízení. Rozlišení procesního postavení jednotlivých subjektů (například obviněný, poškozený nebo svědek) trestního řízení je nezbytné pro určení a výkon práv dle trestního řádu.“[21]

Podle **§ 27** má subjekt právo na získání informací o identitě správního orgánu, o adresních údajích, kdy se může obrátit na pověřence pro ochranu osobních údajů a jejich účelu zpracování, případnému právu na podání stížnosti k Úřadu a kontaktní údaje Úřadu a právu subjektu údajů na případný přístup k osobním údajům, jejich opravě nebo k jejich omezení

[20] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 79.

[21] VLACHOVÁ, Barbora, MAISNER, Martin. Zákon o zpracování osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2019, 168 s. ISBN 978-80-7400-760-6, s. 61.)

zpracování, nebo pro výmaz osobních údajů. Spravující orgán má za povinnost zveřejnit tyto informace snadno přístupným, srozumitelným způsobem umožňujícím dálkový přístup, tj. na internetových stránkách.

V **§ 28** v odstavci 1 je vymezeno právo subjektu údajů na přístup k osobním údajům zpracovaných a vztahujících se k jeho osobě, o rozsahu informací a povinnosti tyto informace spravujícím orgánem poskytnout. Zde je velmi důležité, aby byl subjekt údajů důvěryhodným způsobem identifikovatelný a nedošlo k možnému zaměnění osoby, nebo poskytnutí osobních údajů jiným osobám. V odstavci 2 je vymezeno právo subjektu údajů na přístup, určuje důvody, v rámci kterých je možné poskytnout pouze částečný přístup, popřípadě žádosti nevyhovět. V následujících odstavcích je stanoveno zajištění následné zpětné kontroly, kdy spravující orgán vede o důvodech pro postup podle odstavců 2 a 3 příslušnou dokumentaci, kdy tuto dokumentaci je nutné zachovávat po dobu nejméně 3let.

§ 29 konkretizuje právo na výmaz, opravu a omezení zpracování osobních údajů, jejich vzájemných vztahů a upravuje důvody, pro které nelze těmto žádostem vyhovět.

Následující **§ 30** stanovuje povinnost správního orgánu vyřídit žádost subjektu údajů o právo na přístup, omezení zpracování, opravu, výmaz osobních údajů bez zbytečného odkladu, nejdéle však do 60 dnů ode dne podání. Spravující orgán není povinen žádosti vyhovět, pokud je zjevně nedůvodná, nepřiměřená nebo pokud se ve stejné věci krátce po sobě opakuje. Zákonodárce ani směrnice Evropského parlamentu a Rady (EU) 2016/680 nemá přesně stanovenou dobu, za jak dlouho je možné podat žádost znovu, platí zde tedy obecné pravidlo, kdy zneužití práva nepožívá ochrany. Ustanovení se tímto brání zlomyslnému, opětovnému podávání žádosti v krátkodobém intervalu, ve stejné věci. Pokud je žádosti v plném rozsahu vyhověno, není nutné odůvodnění spravujícím orgánem. Pokud se žádosti nevyhovuje nebo vyhovuje jen částečně, je povinností spravujícího orgánu své rozhodnutí odůvodnit.[22]

§ 31 představuje podnět subjektu údajů o přezkumu zákonnosti zpracování Úřadu pro ochranu osobních údajů a okolnostem, za kterých je možné těmto požadavkům nevyhovět.

[22] Tomuto ustanovení se bude autorka věnovat zvlášť v jiné části práce, neboť se jej dotýká zásadní rozhodnutí Nejvyššího správního soudu

V **§ 32** jsou **taxativně vymezeny základní povinnosti spravujícího orgánu**, včetně technicko-organizačních opatření pro zajištění ochrany osobních údajů. Povinnost uchovávat dokumentaci na přijatá opatření k zajištění ochrany osobních údajů, po dobu zpracování osobních údajů má za úkol spravující orgán. Spravující orgán má za povinnost vedení písemného přehledu o typových činnostech zpracování. Záznam má za úkol doložit plnění povinností v oblasti ochrany osobních údajů pro případnou kontrolu ze strany Úřadu pro ochranu osobních údajů.

Záznam musí obsahovat:

- název a kontaktní údaje spravujícího orgánu a jeho pověřence
- účel zpracování osobních údajů
- kategorie příjemců nebo budoucích příjemců
- kategorie subjektů údajů a kategorie osobních údajů
- informace, zda je použito profilování
- kategorii přenosů do třetích zemí nebo mezinárodních organizací
- právní základ pro operace zpracování, pro něž jsou osobní údaje určeny
- lhůty pro výmaz nebo přezkum potřebnosti kategorií osobních údajů
- obecný popis zabezpečení osobních údajů

*„**Záznamy o činnostech zpracování** je nutno odlišit od tzv. logů, tedy záznamů v systémech automatizovaného zpracování zachycující aktivitu uživatele v konkrétní aplikaci či databázi. Záznamy o činnosti tedy nejsou popisem nějaké (nebo každé) operace zpracování, tj. každého úkolu, který lze s osobním údajem provést, ale o souhrnné záznamy o tom, jak probíhají určité typy zpracování, např. zpracování osobních údajů pro účely budoucí identifikace.“* [23] Následující odstavec upravuje postup spravujícího orgánu dojde-li k nesprávnému předání nebo k předání nesprávných osobních údajů.

§ 33 zahrnuje možnost uzavření písemné dohody pro dva i více spravujících orgánů, které si na jejím základě stanoví společné cíle a prostředky zpracování osobních údajů.

[23] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 97.

Následující paragrafy, **§ 34** a **§ 35** se týkají náležitostí zpracovatelských smluv i povinností zpracovatele k vedení písemného přehledu o typových činnostech zpracování osobních údajů. Je zde vymezen pojem zpracovatel.

Zpracovatelem se rozumí *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt odlišný od správce, který zpracovává osobní údaje správce, místo něj či spolu s ním.“* [24] V navazujícím paragrafu je řešena závaznost pokynů spravujícího orgánu.

Automatizované pořizování záznamů je zpracováno v **§ 36,** který upravuje archivaci logů, tj. konkrétních záznamů o jednotlivých operacích při automatizovaném zpracování osobních údajů za účelem zpětné kontroly zákonného nakládání s osobními údaji, ale i určení osob, které s osobními údaji nakládaly. Dále upravuje uchování osobních údajů do jejich výmazu, a to po dobu maximálně 3 let.

K posouzení vlivu na ochranu osobních údajů slouží **§ 37**, ve kterém spravující orgán zhodnotí plánované zpracování osobních údajů z pohledu uplatněných systémů v průběhu těchto operací, zároveň popsal případná nebezpečí, která mohou při zpracování nastat. *„Správce tedy musí vzít vždy v úvahu taková znevýhodnění subjektu údajů, která nejsou legitimním a záměrným důsledkem zpracování, ale mohou být např. způsobena zneužitím údajů, jejich neoprávněným zpracováním, jejich únikem kvůli nedostatečnému zabezpečení atd.“*[25]

Na **zabezpečení osobních údajů** je kladen velký důraz a orientuje se na něj následný **§ 40**. Spravující orgán, ale i zpracovatel musí přijmout odpovídající opatření na zajištění ochrany zpracování osobních údajů. Konkrétní organizační a technická opatření vychází z povahy, rozsahu okolností, účelu a rizik vznikajících v průběhu zpracování údajů. Opatření tedy vyplývají ze zhodnocení rizik, která hrozí při protiprávní či náhodné likvidaci těchto údajů a případné ztrátě, odcizení, zneužití či neoprávněnému zpracování osobních údajů. Vzhledem k povaze spravujících orgánů se vydávají interní předpisy upravující účinné zabezpečení automatizovaných systémů, ale i nakládání s osobními údaji, zejména ve

[24] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 100.
[25] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 105.

vztahu k určitým osobám. Prioritou je především zamezení zpracování osobních údajů neoprávněnými osobami, zejména tedy to, aby k osobním údajům přistupovali pouze ti zaměstnanci spravujícího orgánu, kteří k tomu mají objektivní důvod vycházející z předmětu jejich činnosti a následných kroků v oblasti fyzické a administrativní bezpečnosti, ale i spolehlivý způsob archivace či skartace dokumentů nebo jiných nosičů dat.

Ohlašováním porušení zabezpečení osobních údajů se zabývá **§ 41**, který je v zákoně o zpracování osobních údajů definován prostřednictvím § 24 odst. 2, tj. odvolávající se na čl. 4 odst. 12 Nařízení, která zahrnuje stejnou definici jako čl. 3 odst. 11 směrnice 2016/680. Jak dále uvádí Nulíček, 2018, k čl. 4, čl. 33 a čl. 34. *Porušením zabezpečení se rozumí „porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, zničené či neoprávněnému poskytnutí nebo zpřístupnění předávaných, uložených nebo jinak zprostředkovaných osobních údajů.“* Porušení zabezpečení je nutné hlásit Úřadu pro ochranu osobních údajů. Zpracovatel má za povinnost toto narušení zabezpečení ohlásit spravujícímu orgánu bez zbytečného odkladu. Spravující orgán by měl uskutečnit ohlášení do 72 hodin od doby, kdy bylo toto porušení zabezpečení zjištěno.

Oznamováním porušení zabezpečení osobních údajů subjektu údajů se zabývá **§ 42**, který ukládá „ *povinnost informovat o porušení zabezpečení osobních údajů subjektu údajů v případech, kdy je shledáno vysoké riziko neoprávněného zásahu do jeho práv a svobod. Informování musí proběhnout bez zbytečného odkladu, což má dodatečným subjektům údajů zejména umožnit včas přijmout nezbytná opatření ke své ochraně.“*[26] Zde se především vychází z toho, že riziko je odvozeno od výše újmy, proto se neopakuje doslovné znění směrnice Evropského parlamentu a Rady EU 2016/680. Je důležité, aby v oznámení spravující orgán uvedl popis povahy zabezpečení, údaje týkající se pověřence, či jiného pracoviště, které může podat podrobnější informace k porušení zabezpečení údajů, podrobný popis případných následků porušení zabezpečení údajů pro subjekt údajů a soupis opatření směřující k nápravě či zmírnění způsobené újmy.

[26] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. Zákon o zpracování osobních údajů. Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 117.

4.2.1.4. Hlava IV – Ochrana osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky

Tato hlava vymezuje podmínky pro zpracování osobních údajů ve vztahu k bezpečnostním a obranným zájmům státu.

Ustanovení výše uvedené Hlavy IV je podle **§ 43** aplikováno na zpracování osobních údajů zajišťující obranné a bezpečnostní zájmy České republiky se týká každého zpracování osobních údajů zpravodajskými službami.
V těchto případech, společně se zpracováním, které provádějí zpravodajské služby, se tato konkrétní úprava výslovně uvádí jako podpůrná k speciální úpravě, kterou obsahují jiné právní předpisy, jako např. zákon č. 153/1994 Sb., o zpravodajských službách České republiky. Mimo zpracování osobních údajů vykonávaného zpravodajskými službami jsou zahrnuty do oblasti Hlavy IV další zpracování, ve kterých to je opodstatněné předmětem, účelem nebo průběžnými okolnostmi možného ohrožení. Národní bezpečnostní úřad zpracovává osobní údaje na základě zákona č. 412/2005 Sb., o ochraně utajovaných informací. Využívání specifických prostředků k získávání informací, následná evidence údajů o osobách monitorovaných Bezpečnostní informační službou případně Vojenským zpravodajstvím a příslušníků zpravodajských služeb (jejich služebních poměrů) jsou upraveny zvláštními zákony, zákon č. 154/1994 Sb., o Bezpečnostní informační službě.

V **§ 44** jsou upraveny **náležitosti zpracovatelské smlouvy**, kdy smlouva musí být uzavřena mezi správcem a zpracovatelem, pokud tento vztah nevyplývá přímo ze zákona. Smlouva musí obsahovat rozsah a účel zpracování, dobu platnosti, ale i důvody vedoucí k uzavření této smlouvy. Následně musí být provedeno dostatečné zabezpečení osobních údajů, kdy úkolem zpracovatele je přijetí dostatečných záruk i následných kroků pro zabezpečení dat. Odpovědnost zpracovatele má zajistit **§ 45**, kdy zpracovatel zpracovává osobní údaje pro správce na základě zákona nebo smlouvy podle § 44 a má za povinnost poukázat na případná pochybení, ke kterým při zpracování osobních údajů dochází a která opět vyplývají ze zákona o zpracování osobních údajů, nebo zvláštního právního systému upravujícího spolupráci. Zpracovatel odpovídá za způsobenou škodu společně a nerozdílně se správcem.

Povinnostmi osob při zajištění bezpečnosti osobních údajů v **§ 46** formou přijetí technických a organizačních opatření, jako jeden z možných základů ochrany osobních údajů, kdy tato hlavní zásada se projektuje do povinností správce, který se řídí Hlavou IV. Je nutné, aby správce i zpracovatel ze zákona přijal veškerá vhodná technická a organizační opatření k řádnému nakládání s osobními údaji. Povinností správce je, aby o přijatých opatřeních vedl příslušnou dokumentaci. Tímto je zajištěno zabezpečení osobních údajů u osob, které k nim přistupují.

V **§ 47** je stanovena **povinnost mlčenlivosti**, „ *že každý, kdo se seznamuje s osobními údaji (zaměstnanci správce či zpracovatele, jiné osoby), je povinen zachovávat mlčenlivost jak o osobních údajích, s nimiž se seznámil, tak o organizačních a technických opatření, pokud by jejich zveřejnění ohrozilo bezpečnost osobních údajů*.“[27] Povinnost mlčenlivosti trvá i po skončení pracovního poměru, nebo jiné obdobné činnosti. V dalším **§ 48** jsou stanoveny podmínky pro výmaz osobních údajů, kdy správce zpracovává osobní údaje za určitým účelem. Zde má být zaveden systém umožňující výmaz nepotřebných osobních údajů. Výmaz obsahuje jak skartaci dokumentů, tak i odstranění osobních údajů z automatizovaných systémů. V **§ 49** jsou stanovena práva subjektů údajů, srovnatelná obecným právům subjektu údajů podle Nařízení Evropského parlamentu a Rady EU 2016/680, *„tedy právo požadovat vysvětlení, opravu nepřesně zpracovaných osobních údajů, výmaz nebo jejich doplnění, a to tedy, pokud ke zpracování dochází v rozporu s ochranou soukromého a osobního života subjektu údajů nebo s ustanoveními Hlavy IV.“*[28] V tomto případě se tedy subjekt údajů může na správci nebo zpracovateli domáhat ochrany svých práv, avšak v omezenějším rozsahu, než je podle Nařízení Evropského parlamentu a Rady EU 2016/680, nebo podle Hlavy III, běžné.

[27] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 128.
[28] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. Zákon o zpracování osobních údajů. Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 130.

4.2.1.5. Hlava V – Úřad

Hlava V se zabývá působností, postavením, složením a pravomocemi **Úřadu pro ochranu osobních údajů**. Zároveň určuje skutečnost, že Úřad má pravomoc k projednání přestupků a ukládání pokut. Jelikož se autorka činnosti Úřadu již v této práci věnovala, podrobí následující ustanovení pouze stručné analýze.

§ 50 zřizuje Úřad pro ochranu osobních údajů, ve kterém jsou mu svěřena oprávnění dozorového úřadu v rámci čl. 51 Nařízení. Tento dozorový úřad byl zřízen zákonem o ochraně osobních údajů v roce 2000 a nedošlo u něj k žádné změně, a to ani v důsledku adaptace Nařízení.
Úřad pro ochranu osobních údajů má své kompetence, které jsou prioritně dány zákonem o zpracování osobních údajů a především dozorem nad touto ochranou. Další předpisy upravují kompetence Úřadu např. v oblasti základních registrů, o střetu zájmů, nakládání s identifikačními doklady a etc.

Nezávislost dozorového orgánu pro ochranu dat, kterým je Úřad pro ochranu osobních údajů je upravena v ustanovení **§ 51**. Tato nezávislost je stanovena článkem 52 Nařízení, které ho upravuje na podmínky českého právního řádu a ústavního pořádku.
Nezávislost je možné rozdělit do tří složek, kterými jsou:

1. **Funkční nezávislost -** Zde je důležité, aby Úřad nebyl nikomu podřízen a další orgány státní správy jej nemohly instruovat, jakým způsobem má vykonávat své úkoly.
2. **Materiální nezávislost -** Rozpočet Úřadu pro ochranu osobních údajů vytváří nezávislou složku státního rozpočtu.
3. **Personální nezávislost** - Úřad řídí předseda, který je jmenován na 5 let, maximálně dvakrát po sobě. Předseda musí být bezúhonnou osobou, která nezastává žádnou veřejnou funkci (poslanec, senátor, soudce apod.) ani nesmí být členem politické strany nebo politického hnutí.

Závěrečný odstavec řeší především ten fakt, že vůči rozhodnutí předsedy Úřadu ve věci státní služby a proti rozhodnutí kárné komise Úřadu, není možné odvolání.

V následujícím **§ 52** a **§ 53** jsou definovány zákonné podmínky, které musí osoby stojící v čele dozorového úřadu splňovat.

V § 54 jsou upřesněny podmínky činnosti dozorového orgánu a vyplývající kompetence za účelem prevence, vyšetřování, odhalování a stíhání trestných činů nebo výkonu trestů v rámci trestněprávní směrnice. Při výkonu dozoru se Úřad řídí nařízením (EU) 2016/679 (obecné nařízení o ochraně osobních údajů) a zákonem č. 110/2019 Sb., o zpracování osobních údajů. Správní dozor je rozdělen do dvou fází, kterými jsou fáze zjišťování a hodnocení (výkon kontroly) a fáze aplikace nápravných nebo sankčních prostředků (fakultativní fáze), která závisí na výsledku zjištění a hodnocení. Podle § 54 odst. 2 písm. d) Úřad pro ochranu osobních údajů projednává přestupky a ukládá pokuty.

Následující **§ 55** upravuje využití registru obyvatel, ale i údajů z informačních systémů evidence obyvatel nebo i cizích státních příslušníků. V **§ 56** je především upravena mezinárodní spolupráce při dozoru nad zpracováním osobních údajů v trestněprávní oblasti. Navazující **§ 57** se týká zákonné povinnosti vypracovat výroční zprávu za předcházející kalendářní rok.

Oprávnění Úřadu na přístup k informacím upravuje **§ 58**, kdy je Úřad oprávněn seznamovat se se všemi informacemi nezbytnými pro plnění konkrétního úkolu. Toto ustanovení v odst. 1 prolamuje povinnost mlčenlivosti podle jiného právního předpisu (např. zákona o advokacii). Ust. § 58 dále rozvádí, za jakých podmínek se může Úřad seznamovat s informacemi chráněnými povinností mlčenlivosti (např. přítomnost a souhlas zástupce Advokátní komory, Komory daňových poradců). Informace, se kterými se Úřad pro ochranu osobních údajů seznamuje při vykonávání dozoru, lze rozdělit do pěti skupin :

- Informace bez speciální zákonné ochrany, ke kterým má Úřadu pro ochranu osobních údajů umožněn přístup.
- Informace chráněné zvláštní povinností mlčenlivosti podle zvláštního právního předpisu.
- Informace nebo dokumenty chráněné zvláštní povinností mlčenlivosti s doplňujícím výpisem subjektů, kterým mohou být tyto konkrétní informace přístupné.
- Informace použité v některých specializovaných oblastech, např. advokacie.

- Informace utajované na základě zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

V **§ 59** je upravena povinnost mlčenlivosti pro místopředsedy a zaměstnance Úřadu. Tito musí zachovávat mlčenlivost o skutečnostech, se kterými se při plnění výkonu působnosti Úřadu pro ochranu osobních údajů seznámí. Může se tedy jednat o osobní údaje, ale i o údaje chráněné zvláštními zákony, jako např. zákonem č. 121/2000 Sb., autorským zákonem, nebo dalšími organizačními a technickými opatřeními. Tato povinnost mlčenlivosti trvá i po skončení služebního nebo pracovního poměru, není tedy časově omezená.

Jako poslední v Hlavě V je ust. **§ 60**, které se týká opatření k odstranění nedostatků, pokud Úřad pro ochranu osobních údajů zjistí *„porušení povinností vyplývajících z tohoto zákona, ať už při zpracování v režimu Nařízení a adaptovaném v Hlavě II zákona o zpracování osobních údajů, nebo zpracování dle směrnice 2016/680, která je transponována v Hlavě III zákona o zpracování osobních údajů, může příslušnému správci či zpracovateli osobních údajů, u kterého porušení zjistí, uložit opatření k odstranění nedostatků včetně lhůty.“*[29] Opatření je nařízeno běžným správním rozhodnutím v souladu se správním řádem.

4.2.1.6. Hlava VI – Přestupky

Hlava VI, se týká zvláštních přestupků za porušení zákazu zveřejnění osobních údajů podle jiných právních předpisů, např. zákona o č. 218/2003 Sb., o soudnictví ve věcech mládeže, ve znění pozdějších předpisů. Dále konkretizuje fakt, kdy porušení obecného nařízení je přestupkem, a upřesňuje okolnosti, za kterých se může fyzická či právnická osoba přestupku dopustit. Stanovuje též přestupky za porušení proti Hlavě III. A zároveň Úřadu dává za úkol upustit od uložení pokuty za možné porušení povinností orgánům veřejné moci a veřejným subjektům.

[29] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. Zákon o zpracování osobních údajů. Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 161.

Podle právní zásady **"Nullum crimen sine lege, nulla poena sine lege"** je pro vymahatelnost zákonem daných povinností nutné stanovit, co je porušením zákona, resp. deliktním jednáním (přestupky a trestné činy, které se dělí na přečiny, zločiny nebo zvlášť závažné zločiny) a jaký je trest za takové porušení. Výše uvedená zásada v rozšířeném chápání znamená, že bez přesného určení, že nějaké jednání je deliktní a že za něj hrozí trest, je jakékoliv uložení povinnosti "bezmocné", neboť teprve hrozba sankcí má dostatečně preventivní charakter. Obecným předpisem, který stanoví, co je přestupek, je zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, který ust. § 5 definuje termín **přestupek** jako *"společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin."*[30] **Společenská škodlivost** je podstatným znakem přestupku. Musí být samozřejmě naplněny znaky přestupku, tedy formální znaky (popsané zákonem), ale zároveň i materiální znaky přestupku - minimálně **ohrožení** právem chráněného zájmu, pokud nedojde rovnou k **porušení,** aby se jednalo o přestupek. Tento zákon poskytuje obecnou úpravu přestupků a upravuje specifika přestupkového řízení. Zákon o zpracování osobních údajů pak v hlavě VI říká, jaké jednání (či opomenutí) je protiprávní, tedy přestupek, přičemž se tím opírá o obecnou úpravu zákona o přestupcích.

Přestupky proti zákazu zveřejnění osobních údajů se zabývá **§ 61** který bere v úvahu možnost porušení zákazu zveřejnění osobních údajů ze strany fyzických osob, díky kterému se dopouštějí přestupku. Za spáchání přestupku uvedeného v tomto paragrafu lze uložit pokutu až do výše 1.000.000 Kč a v případě zveřejnění těchto údajů v médiích je možné uložení pokuty až do výše 5.000.000 Kč.

Možným přestupkovým jednáním při zpracování osobních údajů u právnických osob se zabývají **§ 62** a **§ 63,** tyto dva paragrafy jsou si velmi podobné. Jediným rozdílem je zde fakt, že v **§ 62** se přestupku dopouští správce nebo zpracovatel a v případě **§ 63** se přestupkového jednání dopouští fyzická osoba. Oba tyto paragrafy však uvádějí výčet možných pochybení při zpracování osobních údajů.

[30] Zákon č. 250/2016 Sb., zákon o odpovědnosti za přestupky a řízení o nich, § 5.

V následujícím **§ 64** se uplatňuje objektivní odpovědnost, proto se tedy nezkoumá zavinění, subjekty zde automaticky odpovídají za způsobený stav. Pokud přestupce věrohodně prokáže, že vyvinul maximální snahu, aby nedošlo k porušení zákona, může Úřad, jemuž toto rozhodnutí náleží, obviněného zprostit odpovědnosti za přestupek.

V některých případech je možné podle **§ 65** jednoduché a neformální řešení přestupků, kterým může být odložení věci. Úřad věc odloží, aniž by zahájil řízení o přestupku, pokud je vzhledem k podmínkám uvedeným v tomto ustanovení zřejmé, že účelu, kterého by bylo možné dosáhnout provedením řízení o přestupku, bylo dosaženo nebo jej lze dosáhnout jinak. Podmínky odložení věci podle tohoto ustanovení se týkají významu a míry porušení nebo ohrožení chráněného zájmu, dále způsobu provedení činu, jeho následku, okolnostem, ale také vzhledem k chování podezřelého po spáchání činu.

„Primárně tak bude tento institut využíván ÚOOÚ v bagatelních případech, kdy bude do soukromí subjektů zasaženo ve velmi malé míře, popřípadě kdy již byla podezřelým ze spáchání činu zajištěna náprava.“[31]
Podmínky, za kterých může dojít k odložení věci, jsou stanoveny dosti obecně, díky tomuto jsou osoby podezřelé ze spáchání přestupku motivovány k nápravě stavu a ke zmírnění případných dopadů porušení zákona o zpracování osobních údajů, ve snaze předejít uplatnění správních sankcí.

Odložení věci bez zahájení přestupkového řízení se uvádí v ust. § 76 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů, a je uplatněno zejména v případě, pokud se o přestupek nejedná. Toto ustanovení nabízí celkem 12 důvodů, za kterých správní orgán věc odkládá, mezi nejdůležitější, dle názoru autorky této práce, patří: a) došlé oznámení neodůvodňuje zahájení řízení o přestupku nebo předání věci, e) podezřelý z přestupku nebyl v době spáchání skutku pro nepříčetnost za přestupek odpovědný, f) odpovědnost za přestupek zanikla, j) o skutku již bylo rozhodnuto jako o disciplinárním deliktu a uložené opatření lze považovat za postačující, a také

[31] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 175.

odst. 2 - Správní orgán, aniž řízení zahájí, věc usnesením odloží, jestliže se o totožném skutku vede trestní řízení.

Zákon č. 110/2019 Sb., zákon o zpracování osobních údajů je „lex specialis“ (speciální právní úprava mající k jiné obecnější právní úpravě přednost, obvykle upřesňuje konkrétní oblast) ve vztahu k zákonu **č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich (přestupkový zákon)**, vyjma odložení věci je důležité zmínit i institut **promlčení podle ust. § 30 přestupkového zákona.**

Pokud dojde k uběhnutí promlčecí doby, aniž by bylo zahájeno ve věci řízení, jak vysvětleno dále, **zaniká** odpovědnost za přestupek. Promlčecí doba je 1 rok nebo 3 roky, pokud se jedná o přestupek s horní sazbou pokuty alespoň100 000,- Kč.

Promlčecí doba podle § 31 zákona o odpovědnosti za přestupky a řízení o nich, začíná běžet od následujícího dne po dni spáchání přestupku, tedy dnem ukončení jednání, kterým byl přestupek spáchán. Je-li znakem přestupku účinek, promlčecí doba začíná běžet dnem následujícím po dni, kdy takový účinek nastal.
Promlčecí doba začíná běžet:

- v případě přestupku následujícím dnem po dni, kdy došlo k poslednímu dílčímu útoku
- v případě hromadného přestupku následujícím dnem po dni, kdy došlo k poslednímu útoku
- v případě trvajícího přestupku následujícím dnem po dni, kdy došlo k odstranění protiprávního stavu.

Zákon v ustanovení § 32 počítá s okolnostmi, za nichž dochází ke **stavení a přerušení promlčecí doby.** Stavení promlčecí doby způsobuje, že po určitou zákonem stanovenou dobu promlčecí doba neběží.
Do promlčecí doby se nezapočítává doba:

- po kterou se pro tentýž skutek vedlo trestní řízení
- po kterou bylo řízení o přestupku přerušeno
- po kterou se o věci vedlo soudní řízení správní
- po kterou trvalo podmíněné upuštění od uložení správního trestu

Přerušení promlčecí doby způsobuje, že začíná běžet nová lhůta pro promlčení přestupku. Promlčecí doba se přerušuje:

- oznámením o zahájení řízení o přestupku
- vydáním rozhodnutí, kdy obviněný je uznán vinným
- vydáním rozhodnutí o schválení dohody o narovnání

Při přerušení promlčecí doby, odpovědnost za přestupek zaniká nejdéle 3 roky od jeho spáchání, pokud se jedná o přestupek s horní sazbou pokuty alespoň 100 000,- Kč, odpovědnost za přestupek zaniká nejdéle 5 let od jeho spáchání.

4.2.2. Část druhá – Přechodná, zrušovací a závěrečná ustanovení

Následující **§ 66** první odstavec podporuje návaznost ve fungování Úřadu pro ochranu osobních údajů, je zde zajištěno nepřekrývání se jednotlivých funkčních období místopředsedů. Dále je ve druhém a třetím odstavci tohoto paragrafu stanoveno, že dosavadní předseda a inspektoři Úřadu pro ochranu osobních údajů dokončí své funkce podle zákona o ochraně osobních údajů a budou do konce svých funkčních období řídit kontroly, které budou moci plnit podle pověření vedení i příslušně kvalifikovaní státní zaměstnanci Úřadu pro ochranu osobních údajů. Ve čtvrtém odstavci je řešen osud registru zpracování osobních údajů, který je upraven v § 35 zákona o ochraně osobních údajů, do kterého se zapisují informace z oznámení k osobám správců podle § 16 odstavec 2 zákona o ochraně osobních údajů. Následný odstavec sjednocuje pojem **„citlivý údaj“**, kdy je zcela jasné, které kategorie osobních údajů ve smyslu Nařízení jsou zařazeny pod pojmem „citlivý osobní údaj“. Takovýmto způsobem je zajištěna vhodná návaznost významu tohoto pojmu a je zamezeno vymizení definice zakotvené v zákoně o ochraně osobních údajů. Oproti zákonu o ochraně osobních údajů je však definice částečně rozšířena, ale i částečně zkrácena. Nově byl původní „údaj o sexuálním životě“ rozdělen na „údaje o sexuálním chování“ a „údaje o sexuální orientaci“, dále jsou citlivé údaje rozšířeny o údaje týkající se rozsudků v trestních věcech a trestných činů nebo souvisejících bezpečnostních opatření, naopak ze zákonné definice zmizela národnost. *„Věcný posun obsahu definice dle § 66 odst. 6 a Nařízení oproti významu definice dle zákona o ochraně osobních údajů je přitom velmi malý, nulová definice podle Nařízení je užší o národnostní původ, naopak je širší v oblasti rozsudků o trestných činech a souvisejících bezpečnostních*

opatřeních a výslovně zahrnuje i sexuální orientaci.“[32] V rámci praktického uplatnění má tato změna definice jen velmi malý vliv.

Předposlední **§ 67** zahrnuje výčet zrušovacích ustanovení a následující poslední § 68 nabytí účinnosti, tedy to, že zákon nabývá účinnosti dnem jeho vyhlášení. V případě zákona číslo 110/2019 Sb., o zpracování osobních údajů, zákon nabyl účinnosti 24.04.2019.

[32] NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. *Zákon o zpracování osobních údajů.* Praha. Wolters Kluwer ČR, 212 s. ISBN 978-80-7598-467-8. str. 181.

5. Aplikace právní úpravy v praxi

Po výše uvedené analýze zákona o ochraně osobních údajů hodlá autorka navázat pojednáním o prolomení ochrany osobních údajů, a to ve veřejném zájmu. Vzhledem k obsáhlým možnostem orgánů veřejné správy, jak ve veřejném zájmu překročit onu pomyslnou hranici, se autorka práce zaměří konkrétně na jeden způsob tohoto „prolomení" - na moderní, a pro mnohé zároveň rozporuplný, kamerový monitoring. Pro komparaci se autorka hodlá věnovat i využití tohoto monitoringu v soukromém sektoru."

V poslední době je v tomto kontextu velmi často používané sousloví "**veřejný zájem**", proto je vhodné úvodem ve stručnosti zmínit, co tento pojem znamená. Pro sousloví veřejný zájem neexistuje žádná zákonná definice. Pro přesnější výklad tohoto pojmu je tedy nutné nahlédnout do judikatury – Nejvyšší správní soud se k veřejnému zájmu staví takto: *„Z povahy věci lze dovodit, že se jedná o takový zájem, který lze označit za obecný či veřejně prospěšný, případně za zájem společnosti jako celku. Takový zájem nemůže být v rozporu s platnými právními předpisy."*[33]

K veřejnému zájmu se vyjádřil též americký politik Lippmann (volně přeloženo): *„Žijící dospělí sdílejí, doufejme, stejný veřejný zájem. Pro ně, nicméně, je veřejný zájem promíchán a často v rozporu, s jejich soukromými a zvláštními zájmy. Takto můžeme říci, tedy navrhuji, aby byl veřejný zájem presumován jako to, co by si lidé vybrali, kdyby viděli jasně, mysleli racionálně, jednali nezainteresovaně a benevolentně."*[34]

Právní teoretik prof. Gerloch definoval v právnickém slovníku veřejný zájem takto: *„druh zájmu, který je obecně prospěšný, opak čistě soukromého zájmu. Uplatňuje se v tvorbě, interpretaci a v aplikaci práva, zvláště jako jeden ze dvou důvodů zákonné limitace základních práv a svobod. Protože se jedná o jeden z právních pojmů s neostrým významem, měl by být v zákonech blíže specifikován či definován."*[35]

---

[33] Rozsudek Nejvyššího správního soudu ze dne 23.10.2003, č.j. 2 As 11/2003-164, [232/2004 Sb. NSS]
[34] LIPPMANN, Walter. Essays in the public philosophy. Boston, Toronto. Little, Brown and Company 1955 s. 42.
[35] GERLOCH, Aleš. Veřejný zájem. In: HENDRYCH, Dušan a kol. Právnický slovník. 3., podstatně rozš. vyd. Praha: C.H. Beck, 2009, 1459 str., ISBN 9788074000591 s. 1236.

Vymezení zákonem chráněného zájmu je důležité zejména v přestupkovém řízení, kdy se řeší jak formální, tak materiální stránka přestupku. Ohrožením (nebo přímým porušením) zákonem chráněného zájmu dochází k naplnění materiální stránky přestupku a jedná se tak již o přestupek, byť nedošlo k těžšímu následku. Analogicky např. v dopravě: Porušení max. rychlosti v obci. Obviněný nezpůsobil žádný těžší následek ve formě nehody či sražení chodce, ale jízdou ve vyšší rychlosti tento zájem (ochrana zdraví a majetku, bezpečnost provozu na silničních komunikacích) pouze ohrozil, přesto však došlo ke spáchání přestupku. Veřejný zájem se dá tedy zpětně odvodit od toho, co která norma chrání. Z příkladu výše uvedeného přestupku v silniční dopravě lze též odvodit, že veřejný zájem a soukromé zájmy jsou často provázané. Soukromým zájmem je zde zdraví případného chodce sraženého motorovým vozidlem, naopak veřejným zájmem je bezpečnost provozu na silnicích. V ideálním světě by byl setřen rozdíl mezi veřejným a soukromým zájmem.

Z výše uvedeného je tedy zjevné, že veřejný zájem není obecným pojmem a bude vždy na individuálním posouzení problematiky, zda je některé jednání ve veřejném zájmu, či nikoliv. Jak bylo avizováno výše, autorka se hodlá věnovat užití kamerových systémů ve veřejném zájmu.

Existují některé subjekty (jako např. Policie ČR, obecní policie, celní správa a etc.), které mají **samostatné povolení ke zpracování osobních údajů** ve zvláštních zákonech. Zde je tedy velmi důležité **rozlišení monitoringu** kamerovým systémem **na základě zvláštního zmocnění,** nebo ostatními správci údajů. Je důležité zmínit, že správcům údajů, kteří neměli oprávnění ze zvláštního zákona, existovala do 25.5.2018 registrační povinnost k ÚOOÚ při provozu kamerového systému, ta však s účinností Nařízení GDPR odpadla.

Zvláštního zmocnění pro zpracování osobních údajů využívá především **Policie České republiky, obecní policie** a mohou tedy, pokud je to nezbytné v rámci plnění jejich úkolů, zpracovávat osobní údaje bez souhlasu subjektu údajů.

Policie České republiky má v §79 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, obsaženou zvláštní úpravu, podle které je oprávněna ke zpracovávání osobních údajů za účelem předcházení, vyhledávání a odhalování přestupků, trestné činnosti, stíhání trestných činů, zajištění veřejného pořádku, bezpečnosti včetně pátrání po osobách, věcech a zajištění bezpečnosti v rámci celé České republiky.

Obecní policie je oprávněna zpracovávat osobní údaje, které potřebuje k plnění úkolů podle § 11a zákona č. 553/1991 Sb., o obecní policii nebo zvláštního zákona. Za předpokladu, že je to potřebné pro plnění úkolů obecní policie podle zákona o obecní policii, nebo podle zvláštního zákona (např. v případě zákona č. 361/2000 Sb., o provozu na pozemních komunikacích, zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich a etc.), je obecní policie oprávněna pořizovat zvukové, obrazové, nebo jiné záznamy z míst veřejně přístupných. Obecní policií současně provozované ve veřejném zájmu **městské kamerové dohlížecí systémy** výrazným způsobem přispívají k plnění úkolů obecní policie**,** a to jak v prevenci kriminality, tak v následném šetření deliktního jednání.

Městem provozované kamerové systémy fungují s využitím k tomu vyškoleného personálu, především z řad policie ČR, městské policie, jiných bezpečnostních sborů.

Městské kamerové dohlížecí systémy *(dále jen „MKDS“) jsou specifickým druhem využití kamerových systémů v protiprávní činnosti nejzatíženějších městech a obcích v České republice, na které jsou uvolňovány státní finanční prostředky. Základní charakteristikou provozování a využívání MKDS je jejich preventivní funkce, tj. vytváření bezpečných zón v exponovaných lokalitách. MKDS jsou instalovány v místech, kde se nejčastěji pohybují obyvatelé a návštěvníci měst, kde jsou koncentrovány kulturní, komerční a společenské instituce a kde jsou dopravní uzly měst, např. náměstí, pěší a obchodní zóny, parkoviště, autobusové či vlakové nádraží, sídliště. MKDS musí monitorovat pouze veřejné prostranství. Tím se rozumí podle § 34 zákona č. 128/2000 Sb., o obcích, všechna náměstí, ulice, tržiště, chodníky, veřejná zeleň, parky, a další prostory přístupné každému bez omezení, tedy sloužící obecnému užívání, a to bez ohledu na vlastnictví k tomuto prostoru.*[36]

Městem provozované kamerové systémy mohou monitorovat pouze veřejná prostranství ve smyslu **zákona č. 128/2000 Sb., o obcích**, kdy míra kriminality by měla být rozhodujícím faktorem pro rozmístění kamer v konkrétní oblasti. Nadále zde platí povinnost, kdy monitorovací pracoviště musí mít vnitřní směrnici monitorovacího pracoviště.

[36] Informace o provozování kamerových systémů. Ministerstvo vnitra, dostupné [online]: http://www.mvcr.cz/clanek/informace-o-provozovani-kamerovych-systemu.aspx Poslední přístup dne 6.2. 2021

Celý komplex směrnic musí stanovit jednoznačná práva a povinnosti personálu ve vztahu k MKDS. Názvy směrnic mohou být různé, ale obsahem musí být zejména následující okruhy problémů:

- *Pracovní náplň obsluhy městského kamerového dohlížecího systému a ochrany osobních údajů, technické možnosti odborného ovládání a nastavování kamer, postup při pozorování scény, relevantní vyhodnocování informací, cílené předávání poznatků kompetentním orgánům.*
- *Odborné ukládání informací – tvorba dokumentace, evidence záznamů, předávání dokumentace, práce a ukládání dokumentace a případná skartace.*
- *Zaškolení obsluhy a její pravidelné průběžné proškolování, úprava vlastního výkonu služby – harmonogram služeb, součinnostní vztahy monitorovacího pracoviště s dalšími subjekty a prvky Integrovaného záchranného systému.*
- *Seznamy oprávněných osob, které mohou vstoupit do prostor režimového pracoviště (obsluha, technici, kontrolní a nadřízené orgány) a dále seznam konkrétních osob, které jsou výlučně oprávněny systém ovládat – ostatní osoby nemají umožněn vstup.*
- *Otázky mlčenlivosti a Kontrolní činnost.*[37]

Strážník obsluhující kamerový systém má povinnost zachovávat **mlčenlivost**, kdy každý strážník je povinen zachovávat mlčenlivost o skutečnostech, se kterými se seznámil v souvislosti s plněním úkolů obecní policie. Tato povinnost je dána § 26 zákona č. 553/1991 Sb., o obecní policii. U policistů povinnost mlčenlivosti vychází z § 115 zákona č. 273/2008 Sb., o Policii České republiky. K pracovněprávním předpisům obecní policie náleží zejména zákon č. 262/2006 Sb., zákoník práce a zákon č. 553/1991 Sb., o obecní policii. U příslušníků Policie ČR řeší tuto oblast zákon o služebním poměru, zákon č. 273/2008 Sb., o Policii České republiky. Zákon o Policii ČR a obecní policii ukládá povinnost nejméně jednou za 3 roky prověřit, zda jsou tyto osobní údaje, které k plnění svých úkolů zpracovává, pro plnění těchto úkolů ještě potřebné. V případě, že jsou již nepotřebné, musí být bez zbytečného odkladu proveden výmaz osobních údajů podle § 48 zákona 110/2019 Sb., o zpracování osobních údajů.

Zásadním průlomem v užívání kamerových systémů ve veřejném zájmu bylo nasazení malých bezpilotních letadel - dronů, opatřených kamerami k pořizování videozáznamů. Od

[37] KONÍČEK, Tomáš. Městské kamerové dohlížecí systémy v praxi obcí a měst v České republice, dostupné [online] http://denik.obce.cz/clanek.asp?id=6737369

roku 2020 nasadila Policie ČR již přes tři desítky dronů do terénu.[38] Drony mohou být vybaveny běžnou kamerou pro pořizování videozáznamu nebo také termovizí, fotoaparátem či jiným technickým zařízením, podle účelu konkrétního dronu.

Drony jsou využívány Policií ČR k veřejno-pořádkovým opatřením, k monitoringu dopravy, ale jsou využívány i během vyšetřování trestných činů, pro činnost cizinecké policie a další činnosti různých oddělení Policie ČR.

Oproti zahraničí je nasazení bezpilotních letadel na našem území značně opožděné. Např. Spojené státy Americké nasadily jen v roce 2020 celkem 1578 jednotek dronů.[39]

S použitím dronů se samozřejmě váže ten samý střet zájmů, jako je u stacionárních kamerových systémů, tedy míra narušení soukromí ve veřejném zájmu. Pozornost ombudsmanky Šabatové si vyžádal incident z roku 2019, kdy dva páry tábořily nelegálně v Brdech, konkrétně v oblasti s možným výskytem vojenské pyrotechniky. Přítomnost tábořících párů byla odhalena za použití dronu, a právě jeho použití (vyjma terminologického sporu o to, co je bivakování a co je táboření) se stalo předmětem stížnosti k ombudsmance. Veřejná ochránkyně práv však neshledala pochybení na straně Policie ČR, ale to však za situace, kdy hlídka přítomná v blízkosti tábořiště nabyla dojmu, že v dané oblasti někdo táboří, ještě před vysláním dronu. Samotný dron byl pak použit pouze k ověření předpokladu hlídky.

„V samotném používání dronů, coby moderního prostředku, který významným způsobem zvyšuje efektivitu práce při dohledu nad dodržováním právních předpisů, mohu jen stěží spatřovat něco protiprávního, nejde-li o systematický či nepřiměřený zásah do soukromí osob. “[40]

Veřejná ochránkyně práv se v citovaném stanovisku dále vyjádřila, že použití dronu bylo adekvátní, obzvláště za situace, kdy byla monitorována oblast, která požívá vyšší stupeň ochrany, neboť se jedná o chráněnou krajinnou oblast, ve které se zároveň může vyskytovat dosud nevybuchlá vojenská munice. Naopak by považovala za problematické,

---

[38] kpt. Mgr. Lenka Sikorová, mluvčí PČR, dostupné [online] https://www.policie.cz/clanek/vybaveni-letecke-sluzby-pcr-novymi-drony.aspx

[39] CARR, Nancy K., *Programmed to Protect and Serve: The Dawn of Drones and Robots in Law Enforcement,* 86 JOURNAL OF AIR L. & COM. 183 (2021), str. 201, dostupné [online] https://scholar.smu.edu/cgi/viewcontent.cgi?article=4169&context=jalc

[40] Stanovisko veřejné ochránkyně práv ze dne 30.10.2019, č.j. KVOP-47586/2019, dostupné [online] https://eso.ochrance.cz/Nalezene/Edit/7540

pokud by dron byl použit s cíleným záměrem narušit soukromí fyzických osob bez právního důvodu, který však ve výše uvedeném případu zcela jistě existoval.

Legislativně není použití dronů Policií ČR nijak upraveno, vyjma tedy ust. § 76 zákona č. 273/2008 Sb., o Policii ČR, kdy by se bezpilotní letoun dal zařadit pod zabezpečovací techniku určenou k předcházení nebo odstranění ohrožení veřejného pořádku, jakožto podpůrný operativně pátrací prostředek. Dle ust. § 72 je policista oprávněn užít zabezpečovací techniky při předcházení trestným činům, při získávání poznatků o trestné činnosti, v souvislosti s trestním řízením a v souvislosti se zajišťováním krátkodobé ochrany osob. Širší legislativní zakotvení použití dronů v českém právním řádu by bylo na místě, jediným dohledatelným předpisem, který v současné době reguluje lety dronů, je Letecký předpis L2 - Pravidla létání[41], který se vztahuje i na drony, nicméně tento předpis upravuje pouze leteckou dopravu a provoz ve vzdušném prostoru, nikoliv užití dronů Policií ČR ve veřejném zájmu.

Jako příklad neoprávněného použití dronu (resp. použití dronu bez dostatečné opory v právních předpisech) si autorka této práce vybrala zahraniční případ. V souvislosti s protesty proti vládním nařízením v období koronavirové krize ve Francii v první polovině roku 2020 nasadila francouzská policie v Paříži drony k monitorování protestů, resp. k monitorování dodržování sociálního distancingu. Liga lidských práv (League of Human Rights) a asociace La Quadrature du Net napadla užívání dronů, neboť jejich nasazení nemělo oporu ve francouzském právním řádu. Přestože předseda vlády a ministr vnitra argumentovali závažností epidemické situace a nutností kontroly dodržování vládních nařízení, Státní rada Francie dala stěžovatelům za pravdu a svým rozhodnutím (čl. 2) nařídila státu (ministrovi vnitra) bezodkladné zrušení příkazu na používání dronů.[42]

Úřad pro ochranu osobních údajů je v oblasti ochrany osobních údajů **nezávislým dozorovým orgánem**. Je to organizační složka státu, tedy svou podstatou orgán veřejné moci. Tento orgán vytvořil **souhrn pravidel** k nakládání s osobními daty a oprávněné osoby mají za úkol jej dodržovat. Zároveň stanovil i povinnost registrace a nutnosti informovat subjekt záznamu o pořizování záznamu. V roce 2012 tento úřad vydal

[41] Úřad pro civilní letectví, Ministerstvo dopravy České Republiky, *Letecký předpis - Pravidla létání L2,* č.j.: 153/2014-220, dostupné [online] https://aim.rlp.cz/predpisy/predpisy/index.htm

[42] Rozhodnutí Státní rady Francie ze dne 18.5.2020, Nos. 440442, 440445, dostupné [online] https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones

metodiku k provozování kamerových systémů,[43] kde vytýčil základní povinnosti ve snaze tyto povinnosti sjednotit se zákonem.

Obsahem této metodiky je provozování kamerového systému, oznamovací povinnost, dokumentace kamerového systému, dokumentace přijatých technicko-organizačních opatření, udělení souhlasu se zpracováním osobních údajů prostřednictvím kamerového systému, označení prostorů monitorovaných kamerou se záznamem, obsah podrobné informace poskytované subjektu údajů (žadateli), poskytnutí osobních údajů z kamerového systému.

Kamerové systémy lze tedy vnímat také jako oči elektronických zabezpečovacích systémů, které se z velké části tímto přímo podílejí na prevenci a snížení kriminality, nepřetržitě monitorují prostor v jakoukoli denní i noční hodinu, mohou sledovat venkovní, ale i vnitřní prostory, ovládáním na dálku lze měnit jejich zorné pole a obraz lze přenášet prostřednictvím internetové sítě do kteréhokoli místa určení. Přenos prostřednictvím internetové sítě je sice rychlý, zato jsou s ním spojena rizika přístupu nepovolaných osob. Vhodné řešení je uzavřená síť (intranet), do které mají přístup osoby pouze fyzicky přítomné u ovládacího zařízení, nebo patřičná ochrana proti kyberútokům zvenčí ve formě tzv. firewallů a antivirových programů. Z tohoto důvodu jsou při pořizování záznamu kamerovým systémem velmi důležité nejen technické parametry a následná kvalita záznamu, ale především to, jak je s těmito získanými daty posléze nakládáno a jak jsou data primárně chráněna samotným systémem.

Výše uvedené se týkalo zpracování osobních údajů ve veřejném zájmu, jak předpokládá článek 6 odst. 1 písm. e) Nařízení GDPR.

Pro soukromé účely existuje možnost zpracování osobních údajů článek 6 odst. 1 písm. f) Nařízení GDPR, a to za podmínky, že zpracování je nezbytné pro účely **oprávněných zájmů** příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Pod oprávněný zájem se dá subsumovat (ve vztahu k užívání kamerových systémů) zejména ochrana majetku či života a zdraví osob. Správce je oprávněn pořizovat kamerový záznam např. svého rodinného domku a v případě, že je na záznamu zachycen zloděj (tedy

[43] Metodika provozování kamerových systémů vypracovaná ÚOOÚ, dostupné [online] http://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf

fyzická osoba přímo či nepřímo identifikovatelná ze záznamu), smí správce tento záznam předat vyšetřujícímu orgánu. Nesmí však tento záznam využít nijak jinak – nahrání na internet pro pobavení je zakázané, neboť by to bylo již nad rámec primárního účelu pořízení záznamu – ochrany majetku.

K ochraně soukromí se vyjadřuje zejména ust. § 86 zákona č. 89/2012 Sb., občanského zákoníku: *„Nikdo nesmí zasáhnout do soukromí jiného,* ***nemá-li k tomu zákonný důvod.*** *Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou,* ***nebo takové záznamy*** *o jeho soukromém životě* ***šířit****. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.“*

Dalším vhodným příkladem je užití kamerového systému např. na stavbě - zde se může překrývat veřejný i soukromý zájem, neboť zhotovitel stavby (často tedy zaměstnavatel) monitoruje svůj vlastní majetek (např. v současné době velmi drahý stavební materiál), ale zároveň může tento záznam posloužit k ochraně veřejného zájmu - zajištění bezpečnosti a ochrany zdraví na pracovišti (dále jen „BOZP“) ve smyslu zákona č. 262/2006 Sb., zákoníku práce, či zákona č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci, či k případnému objasnění pracovního úrazu. Zaměstnavatel má mnoho povinností, jejichž porušení přímo ohrožuje veřejný zájem, např. kontrolování užívání osobních ochranných pracovních prostředků nebo zamezení vstupu nepovolaných osob do nebezpečného prostoru, čehož může dosáhnout právě pomocí vzdáleného monitoringu, aniž by sám byl přítomen na pracovišti a dodržování předpisů kontroloval fakticky na místě. Informovanosti zaměstnanců o jejich monitoringu se autorka věnuje v následující části práce.

5.1. Problematika monitoringu z důvodu soukromého zájmu

Pro úplnost a komparaci prolomení hranice ochrany osobních údajů z důvodu veřejného zájmu se autorka v další části textu krátce věnuje **zájmům soukromým.**

Hojně diskutované téma poslední doby je **pořizování kamerových záznamů na pracovišti zaměstnavatele**, kdy zaměstnavatelé instalují kamerové systémy v pracovních prostorách s odůvodněním kontroly efektivity pracovního vytížení zaměstnanců nebo za

účelem ochrany svého majetku. Podle zákoníku práce *„zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance* ***otevřenému*** *nebo* ***skrytému sledování****, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.“*[44] Pokud tento závažný důvod není dán, není možné, aby zaměstnavatel zaměstnance monitoroval. Toto není umožněno ani v případě udělení souhlasu zaměstnancem. Na kontrolu pracovní činnost svých zaměstnanců má zaměstnavatel právo, pouze za předpokladu že k tomu využije zákonné prostředky a formy. Zaměstnavatel je tedy oprávněn pořizovat kamerové záznamy jen v případě, kdy sledovaného účelu nelze dosáhnout jinak. Tímto záznamem může být např. kontrola pracovní docházky, dodržení technologických postupů, či zajištění bezpečnosti a ochrany zdraví při práci.

Před účinností nařízení GDPR podléhal provoz kamerových systémů registrační povinnosti, která však již byla ukončena.

Je nezbytně nutné, aby v souvislosti s vyhotoveným návrhem kamerového systému byla správcem vypracována analýza možných variant ochrany sledovaného objektu, osoby nebo zařízení, stejně tak musí být vypracována analýza rizik nebo analýza případných zásahů do soukromí**,** a neméně důležitou je i projektová dokumentace nebo dokumentace technicko-organizačních opatření k provozování kamerového systému.

Dále zde platí povinnost zaměstnavatele splnit informační povinnost vůči subjektům, kterých se to týká. V tomto případě má zaměstnavatel povinnost dotčené osoby informovat o rozsahu, účelu a způsobu zpracování osobních údajů i o tom, jakým způsobem budou zpracovány, případně komu mohou být tyto osobní údaje přístupné. O těchto okolnostech jsou zaměstnanci informováni většinou proti podpisu prostřednictvím interních předpisů zaměstnavatele. Ostatní osoby mohou být vyrozuměny uveřejněním této informace na viditelném místě, např. formou informační tabulky, umístěné na takovém místě, aby se s ní mohla každá přítomná osoba seznámit ještě před vstupem na monitorovaný prostor.

[44] Zákon č. 262/2006 Sb., zákoník práce, § 316 odst. 2

Opět i zde platí pravidlo, že kamerové záznamy se uchovávají pouze po dobu nezbytně nutnou a pokud jsou již nepotřebné, musí být bez zbytečného odkladu provedena jejich likvidace. Pouze v odůvodněných případech, mohou být tyto záznamy předány orgánům činným v trestním řízení. Doba uchování záznamu není zákonem stanovena (zde ale většinou platí nepsané pravidlo tří dnů).

Kamerové systémy nesmí žádným způsobem nadměrně zasahovat do soukromí osob a není tedy možné využívat kamerový systém v místech, ve kterých jsou vykonávány veskrze soukromé úkony. Tímto místem jsou myšleny šatny, koupelny, toalety a etc.

Do problematiky sledování zaměstnanců nejsou zapojeny pouze jen kamerové systémy, ale existuje mnoho jiných možných monitorovacích prostředků a jedním z dalších způsobů sledování je **monitoring služebních vozidel, prostřednictvím signálu GPS (Globální družicový polohový systém).** Tento způsob kontroly je u zaměstnavatelů stále oblíbenějším, poskytuje kompletní přehled o pohybu vozidla, optimalizaci nákladů na provoz, ale i maximální efektivitu využití. Do vozidel je nainstalována monitorovací jednotka tak, aby nebylo možné tuto jednotku svévolně demontovat či poškodit. Díky tomuto systému má pracovník logistiky podrobný přehled o poloze jednotlivých vozidel na mapě, prostřednictvím počítače může kontrolovat styl jízdy a spotřebu u jednotlivých vozidel, případně usměrňovat chování řidičů, pokud by byla jejich jízda agresivní či nehospodárná. Pro řadu firem je velmi důležitou informace, zda jejich zaměstnanci skutečně navštívili všechna místa, která dle plánu měli, případně kde přesně se v danou chvíli nachází kamion s dodávkou zboží pro klienta či zda zaměstnanci neokrádají firmu, nebo nevyužívají vozidla k soukromým účelům.

Z etického hlediska tu však stále existuje nebezpečí, že se sledováním zaměstnanců poruší vyváženost důvěry mezi vedením a zaměstnanci a naruší se tím tak klima ve firmě. Zaměstnanci mohou mít pocit, že jim zaměstnavatel nedůvěřuje a díky tomuto pocitu nedůvěry takovou firmu někteří následně opustí. Je tedy jen na každém zaměstnavateli, pro jaký systém kontroly se rozhodne.

Další neméně důležitou oblastí kontroly ze strany zaměstnavatele může být **monitoring služebních telefonů.** Velká většina zaměstnanců používá služební telefony i pro soukromé účely, ale ne všichni zaměstnavatelé s tím souhlasí. Poslední roky, kdy dominantní roli nad

pevným linkovým telefonem převzal mobilní telefon a ceny telefonních hovorů i díky neomezenému volání jsou velmi nízké, se s nepochopením zaměstnavatele u využití služebního telefonu pro soukromé účely setkáváme již jen velmi zřídka. Může však nastat jiný problém: příliš mnoho soukromých hovorů může narušovat pracovní produktivitu zaměstnance. Dalším problémem dnešní doby může být i fakt, kdy díky existenci tzv. „chytrých mobilních telefonů" může zaměstnavatel opět kontrolovat své zaměstnance vyžadováním zapnutého lokátoru, který je součástí dnes již každého moderního telefonu. Tento lokátor je primárně určen především k nalezení mobilního telefonu při jeho případné ztrátě či odcizení, nicméně zaměstnavatelé tuto funkci využívají i ke sledování svých zaměstnanců. Aktivovaný lokátor vyšle signál přes systém GPS, který je zachycen a zpracován speciální aplikací nainstalované v počítači. Nahlédnutím do této aplikace získá zaměstnavatel velmi podrobný přehled o tom, kdy a kde se jeho zaměstnanec momentálně nachází, a to i zpětně. Zaměřme se tedy na zákonnost výše uvedeného monitoringu. Jednání zaměstnavatele je nutno dát do souvislosti s ust. § 316 zákona č. 262/2006 Sb., zákoníku práce. Odst. 1 citovaného ustanovení **zakazuje zaměstnancům, bez svolení zaměstnavatele,** užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele, včetně **výpočetní techniky nebo telekomunikačních zařízení.** Dodržování tohoto zákazu podle věty první **je zaměstnavatel oprávněn vhodným způsobem kontrolovat.** Dále odst. 2 zakazuje zaměstnavateli, **bez vážného důvodu,** porušit soukromí zaměstnance na pracovišti, ve společných prostorách tím, že by ho podroboval otevřenému nebo skrytému sledování, odposlechu, záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci. Zvláštní povaha činnosti zaměstnavatele (odst.3) však odůvodňuje zavedení mechanismů podle odst. 2, zaměstnavatel je však povinen zaměstnance informovat o rozsahu kontroly a způsobech jejího provádění. Zvláštní povahou činnosti zaměstnavatele pak může být např. zajištění bezpečnosti soudní budovy, kdy justiční stráž provádí bezpečnostní prohlídky u vchodu, a zároveň je tento prostor monitorován, nebo právě výše uvedená kamionová doprava, kdy řidič převáží zboží vyšší hodnoty a ochrana tohoto zboží GPS monitorováním je oprávněným zájmem zaměstnavatele.

Možnost monitoringu e-mailové komunikace v zaměstnání. V dnešní době existují volně dostupné aplikace, díky kterým nadřízený pracovník snadno zjistí, kolik času strávil konkrétní zaměstnanec na internetu. To může být problém, zejména pro toho pracovníka,

který pro výkon svojí práce internet vůbec nepotřebuje. Tento způsob kontroly je možný, jak ostatně potvrdil Nejvyšší soud svým rozsudkem ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011., kdy zaměstnavatel zkontroloval zaměstnance a zjistil, že zaměstnanec se v pracovní době věnoval internetu, a nikoliv práci, kdy za září 2009 strávil tento zaměstnanec přes 102 hodin na internetu, přestože to zaměstnavatel výslovně zakázal ve svém provozním řádu. Celý spor, vedoucí až k judikátu, započal okamžitým zrušením pracovního poměru pro zvlášť hrubé porušení pracovních povinností a věc postupně eskalovala až k Nejvyššímu soudu.

Zatímco zaměstnavatel může kontrolovat dobu strávenou zaměstnancem na internetu, u e-mailu to je trochu komplikovanější. Čtením elektronické pošty zaměstnanců by zaměstnavatel porušil listovní tajemství a dostal by se tak do konfliktu se zákonem. Na tyto případy je pamatováno **Listinou základních práv a svobod**, konkrétně článkem 13: *„Nikdo nesmí porušit **listovní tajemství** ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon.“*[45]

Jak uvádí v článku JUDr. Jouza: *„Zaměstnavatel může kontrolovat elektronickou poštu zaměstnance, jestliže k tomu bude mít závažný důvod spočívající ve zvláštní povaze své činnosti.*[46]*“* K obdobným závěrům dochází i advokát JUDr. Matzner ve svém článku.[47]

Platí tedy, že zaměstnavatel nesmí kontrolovat soukromou e-mailovou schránku svého zaměstnance a seznamovat se s jejím obsahem, takovýmto jednáním by porušil listovní tajemství a právo na soukromí zaměstnance.

Za soukromou e-mailovou schránku se považuje nejen zaměstnancem zřízená e-mailová schránka pro osobní účely, ale i e-mailová schránka zřízená zaměstnavatelem pro zaměstnance za účelem výkonu pracovních činností, v případě že obsahuje zaměstnancovo jméno, např. eva.novakova@zamestnavatel.cz., není tato e-mailová schránka majetkem zaměstnavatele.

---

[45] Ústavní zákon číslo 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů
[46] JOUZA, Ladislav. Právní ochrana elektronické pošty zaměstnanců, [online] dostupné z: https://www.epravo.cz/top/clanky/pravni-ochrana-elektronicke-posty-zamestnancu-112612.html
[47] MATZNER, Jiří. Může zaměstnavatel sledovat vaší aktivitu na internetu nebo pracovní emaily? [online] dostupné z: https://digibiz.cz/muze-zamestnavatel-sledovat-vasi-aktivitu-na-internetu-nebo-pracovni-emaily/

Ale ani v případě bývalých zaměstnanců není možné vstupovat do e-mailové schránky za účelem kontroly e-mailů, toto je přípustné pouze v případě, že zájmy zaměstnavatele převládnou nad právem na ochranu soukromí bývalého zaměstnance a neexistují zde jiné možnosti.

Při dodržení výše uvedených podmínek je možné kontrolu soukromé e-mailové schránky realizovat. Tato realizace je možná pouze způsobem, který v minimální možné míře zasáhne do soukromí bývalého zaměstnance. Kontrolovány tak mohou být např. hlavičky e-mailů, u kterých je zřejmé, že jde o e-maily pracovní povahy a zaměstnavatel je potřebuje z pracovních důvodů prostudovat. S obsahem e-mailů soukromé povahy se tedy zaměstnavatel nesmí v žádném případě seznamovat.

Pokud jde o pracovní e-mailové schránky, na ty se ochrana soukromí nevztahuje a v případě skončení pracovního poměru jejího správce je lze dát bez dalšího do správy jiného zaměstnance. Tyto postupy by měly být upraveny v interní směrnici, díky které bude zajištěna informovanost zaměstnanců o způsobu zacházení s jejich e-mailovými schránkami.

Výše uvedené postupy by měly být v podrobnostech upraveny v interních předpisech. Tím bude mimo jiné zajištěno, že zaměstnanci budou předem a transparentním způsobem informováni o tom, jak bude s jejich e-mailovými schránkami zacházeno.

Z toho tedy vyplývá, že zaměstnavatel u soukromé korespondence může kontrolovat pouze to, od koho a v jakém množství zaměstnanec e-maily dostává nebo komu je píše. U firemní e-mailové schránky to je odlišné. Pokud komunikace s klienty a obchodními partnery probíhá výhradně elektronicky, zaměstnavatel musí mít přístup do firemních e-mailových schránek u všech svých podřízených. Zaměstnavatel má za povinnost své zaměstnance předem informovat o způsobu provádění kontroly, ale i o jejím a rozsahu.

Přestože byla tato část věnována monitorování z důvodů soukromého zájmu zaměstnavatele, lze zde nalézt i přesah do veřejného zájmu, a to zejména u státních zaměstnanců, kdy porušení osobního soukromí, čtení e-mailů a jiný výše uvedený monitoring by mohl být prováděn i ve veřejném zájmu, např. z důvodu odhalování trestné činnosti státního zaměstnance na vysokém postu (zneužití pravomocí úřední osoby) nebo z důvodu prověření řádného chodu různých úřadů.

5.2. Obecná problematika kamerových systémů

Dnes o každém z nás existuje mnoho informací, které se mohou dostat mimo oblast kontroly, často se nám zdá, že jakékoli soukromí už vlastně vůbec neexistuje. V současné době, při pohybu ve městech, je takřka každý náš krok průběžně zaznamenáván kamerovým záznamem. Přestože tyto všední kamerové záznamy nejsou nikde zveřejněny, neobjevují se na internetu, není nám tato skutečnost nikterak příjemná. **Kamerový systém** jako vše na tomto světě má svá **pozitiva**, ale bohužel i **negativa**.

Tím pozitivním důvodem existence a používání kamerových systémů je to, že hlavně přispívá k ochraně, bezpečnosti osob a majetku, dohlíží na dodržování pravidel občanského soužití, veřejného pořádku, napomáhá k odhalování protiprávního jednání a zároveň působí jako prevence před takovýmto jednáním. Přínosů, které může kamerový systém mít je mnoho, jedním z mnoha zásadních pozitiv je zvýšená efektivita ochránců pořádku a s tím související včasná rychlost zásahu, kterým mohou proti narušitelům zakročit, a tedy i případný odrazující efekt na potencionálního pachatele. Kamerový systém nám dokáže zajistit důkazy pro případné ustanovení a usvědčení pachatelů protiprávního jednání a zároveň působí jako důležitý uklidňující prvek pro občany, jako důležitý nástroj pro eliminaci případných nebezpečí. V případě kamerových systémů se může veřejný zájem dostávat do vzájemného konfliktu se zájmem jednotlivce, protože se jedná o protiklad zájmu soukromého, přesahujícího zájem jednotlivce či určité skupiny. V obecné rovině lze tedy veřejný zájem chápat jako zájem podporující rozvoj společnosti, který řeší její konkrétní problémy, např. prostřednictvím kamerových systémů.

A jaká negativa mohou vycházet z využití kamerového systému? Lidem je velmi nepříjemné, pokud jsou sledováni, tento fakt je umocněn i obavou, že zvýšená kontrola a monitoring ze strany státu může negativně ovlivnit svobodu slova a pohybu. Osobám obsluhujícím kamerový systém se dostává rozsáhlé pravomoci a ze strany bezpečnostních sborů nebo jiného provozovatele může dojít ke zneužití informací k vlastnímu prospěchu. Častá však bývá i obava žen ze sledování při návštěvě zkušebních kabinek v obchodě, cestách výtahem, ale i jinde, které trápí představa voyeurismu od osob sledujících obrazovku, známých pod anglickým názvem „peeping Tom“.

Za paradoxní lze ale označit především to, že zejména ti, kterým nejvíce vadí jakýkoli bezpečný monitoring, tak právě tito lidé s naprostým klidem zveřejňují na sociálních sítích

každý svůj krok, různá videa či fotografie, která jsou velmi lehce zneužitelná. Klasickým příkladem mohou být zveřejněné fotografie z právě probíhající dovolené, kdy na základě takto prezentovaných informací může dojít k narušení a možnému vykradení obydlí ještě před návratem z této dovolené. Na základě svých praktických zkušeností jsou tito lidé na jednu stranu k zákonnému systému velmi kritičtí a nedůvěřiví, ale na stranu druhou je jejich jednání dosti krátkozraké a nezodpovědné. Domnívá-li se někdo, že je mu zasahováno do jeho soukromí, má možnost obrátit se na soud s žalobou na ochranu osobnosti a domáhat se, aby bylo upuštěno od neoprávněného zásahu do soukromí nebo aby byl odstraněn následek.

Podobnou možnost pak nabízí v ust. § 49 i zákon o zpracování osobních údajů, kdy může subjekt údajů požádat správce nebo zpracovatele údajů o vysvětlení nebo požadovat odstranění vzniklého stavu provedením opravy, doplněním nebo výmazem a má právo být informován a tomto postupu.

5.3. Kamerové systémy v bytových domech

V této kapitole autorka hodlá provést komparaci klasického veřejného monitoringu, a toho soukromého, protože především povědomí široké veřejnosti je zažitá představa, že pokud se jedná o kamery umístěné v soukromých prostorech, jsou tyto kamery soukromé a ve veřejných prostorech veřejné, to však není úplně pravda. Mnoho soukromých kamer monitorujících veřejná prostranství, zejména jedná-li se o kamery instalované na soukromých domech a částečně snímající prostory mimo obydlí. Článek 6 GDPR, jak již bylo v této práci zmíněno, umožňuje využití kamerového systému, pokud jde o zpracování údajů nezbytné pro účely oprávněných zájmů příslušného správce. Je zcela nesporné, že ochrana majetku a bezpečnosti v bytových domech je považována za oprávněný zájem.

S instalací průmyslové kamery na domě se pojí řada povinností. Velmi důležité je nastavení kamerového systému, je zapotřebí brát v úvahu seřízení zorného úhlu kamery především to, aby minimálně zasahovala do soukromí osob, které jsou kamerami nahrávány. Z tohoto důvodu byl Úřadem pro ochranu osobních údajů zveřejněn seznam míst vhodných k umístění kamerových systémů. Těmito prostory jsou např. sklepy, půdy, garáže, schránky etc., dále mohou být kamery umístěny u vchodových dveří, schodišť a výtahů. Komplikací však může být vnější strana budovy, kde kamerový systém nesmí

nahrávat veřejné prostory, kterými jsou ulice nebo chodníky. Problematické ale může být monitorování vchodů ke konkrétním bytovým jednotkám, kdy v tomto případě dochází k zásadnímu narušení soukromí nejen u osob, které tyto byty obývají, ale i u osob, které tyto byty navštěvují. Před spuštěním kamerového systému je zapotřebí, aby všichni obyvatelé domu byli **podrobně informováni** o tom co, proč, kde a jakým způsobem bude pořizován záznam. Dále je nutné zajistit souhlas všech obyvatel domu ještě před spuštěním kamerového systému, i když tento souhlas není bezpodmínečně nutný. Tento souhlas může být získán právě na členské schůzi příslušného **družstva** nebo **společenství vlastníků** (SVJ), kde všichni, kteří dům obývají, mohou tento souhlas podepsat. Do prostoru, ve kterém je kamerový systém nainstalován, je nutné viditelně umístit informační tabulku s upozorněním pro případné návštěvníky. Neméně důležitým je i důkladné zajištění záznamového zařízení i přístupů k systému proti případnému úniku informací. Dále je nutné akceptovat i tu skutečnost, že osoba zpracovávající data bude mít přístup k citlivým údajům proto v tomto případě je vhodné přizvat k řešení implementátora, který má odbornou kvalifikaci doloženou evropskými certifikáty a odbornou znalost práva.

Zároveň je důležité, aby mezi **správcem osobních údajů** a případným **zpracovatelem osobních údajů** (může jím být i najatá správní firma) byla uzavřena smlouva o jejich zpracování. Tato smlouva by měla obsahovat rozsah, účel a časový úsek, na který se uzavírá, smlouva musí obsahovat i záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů. V případě GDPR toto zpracovává článek 28 odst. 3., který zároveň ukládá další podmínky, jako např. zpracování osobních údajů na základě doložených instrukcí správce, zajištění toho, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, aby se na ně vztahovala zákonná povinnost mlčenlivosti, poskytnutí správci veškerých informací potřebných k dosvědčení toho, že byly splněny všechny potřebné náležitosti. Pokud jsou dodrženy všechny tyto kroky, nic už nebrání bezproblémovému využívání kamerového systému v bytovém družstvu či ve společenství bytových jednotek. Přestože jsou po většinu času zpracovávány osobní údaje obyvatel domu, je zcela nepochybné, že i toto zpracovávání údajů v soukromé sféře má přesah do veřejného monitoringu, neboť z hlediska trestné činnosti má přítomnost kamerového systému, byť soukromého, preventivní charakter a v případě dokonané trestné činnosti v monitorované oblasti lze pořízený záznam využít pro účely prošetření, a je tedy chráněn

veřejný zájem - bezpečnost majetku, zdraví, života obyvatel daného domu, ale zároveň i veřejný pořádek (ve smyslu prevence kriminality).

V závěrečném porovnání lze tedy uvést, že v případě **klasického veřejného monitoringu** mají některé subjekty (Policie ČR, obecní policie, celní správa...) samostatné povolení ve zvláštních zákonech a pro **soukromý monitoring** již není nutná registrace u Úřadu, jako tomu bylo do 25.5.2018.

Zvláštního zmocnění pro zpracování osobních údajů využívá především Policie České republiky a obecní policie, díky němuž mohou, v rámci plnění úkolů, monitorovat veřejná prostranství a následně zpracovávat osobní údaje bez souhlasu subjektu údajů.

V případě soukromého monitoringu je nutno zmínit, že Úřad **považuje provoz kamerového systému za zpracování osobních údajů**, pokud je automatizovaně prováděn záznam monitorovaného veřejného prostoru (jímž může být i chodník před domem) a zároveň je účelem pořizovaných informací a záznamů využití k identifikaci fyzických osob v souvislosti s určitým jednáním.

Závěrem k této části je nutno uvést, že soukromý monitoring lze těžko považovat za čistě soukromý, neboť přestože je často vytvořen k naplnění soukromých zájmů, takřka vždy bude účel monitoringu alespoň částečně prolamovat hranici směrem k zájmu veřejnému, jak bylo demonstrováno na příkladech výše.

5.4. Judikatura vztahující se ke zpracování osobních údajů

Vzhledem k tomu, že zákon o zpracování osobních údajů je doposud velmi nový, je k tomuto zákonu dostupné jen velmi málo konkrétní judikatury. Pro případnou ilustraci alespoň jeden případ, týkající se usnesení Městského soudu v Praze ze dne 21.7.2020, č.j. 3 A 77/2020 – 67 a kasační stížnosti proti tomuto usnesení. V řízení před Městským soudem byla **žalována Česká republika,** za niž v řízení vystupovala Policie České republiky, Ředitelství služby cizinecké policie, se sídlem Olšanská 2176/2, Praha 3**,** a celý případ se na konci minulého roku posunul až k řízení o kasační stížnosti před Nejvyšším správním soudem, vedeném pod sp.zn. 4 Azs 246/2020.

Uvedený judikát je pro tuto práci podstatný, neboť Nejvyšší správní soud po procesním pochybení Městské soudu v Praze **označil** přípis žalované o odmítnutí poskytnutí

informací **za rozhodnutí, a poukázal na mezery zákona č. 110/2019, které vznikly při transpozici GDPR. co se týká opravných prostředků.**

Žalobce podal na zastupitelském úřadě v Káhiře žádost o krátkodobé schengenské vízum za účelem turistickým. Zastupitelský úřad žádost zamítl s odůvodněním, že některý z členských států Evropské unie považuje žalobce za hrozbu pro **veřejný pořádek, vnitřní bezpečnost, veřejné zdraví nebo mezinárodní vztahy**, **rozhodoval tedy ze svého pohledu ve veřejném zájmu**. Žalobce požádal Ministerstvo zahraničních věcí České republiky o nové posouzení důvodů neudělení víza. Ministerstvo rozhodnutím tuto žádost zamítlo s odkazem na závazné stanovisko žalované. Následně žalobce požádal žalovanou v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto osob a o zrušení směrnice 95/46/ES obecné nařízení o ochraně osobních údajů, a se zákonem č. 110/2019 Sb., o zpracování osobních údajů, o sdělení o tom, kterým či kterými členskými státy je považován za hrozbu pro veřejný pořádek, vnitřní bezpečnost, veřejné zdraví nebo pro mezinárodní vztahy jednoho nebo více členských států, za jakou z těchto hrozeb je konkrétně považován, tj. zda za hrozbu pro veřejný pořádek, vnitřní bezpečnost, veřejné zdraví či pro mezinárodní vztahy a z jakého důvodu je za takovou hrozbu považován.

„Na tuto žádost reagovala žalovaná přípisem (sdělením) ze dne 21. 5. 2020, č. j. CPR-1452- 2/ČJ-2020-930320, v němž uvedla, že „podle § 166 zákona č. 326/1999 Sb., o pobytu cizinců je vydávání krátkodobých víz pro území České republiky v gesci Ministerstva zahraničních věcí ČR, a proto v dané věci doporučila obrátit se na Vízový odbor Ministerstva zahraničních věcí ČR."[48]

Žalobce napadl tento přípis žalované žalobou u Městského soudu v Praze (dále jen „městský soud"), ten však usnesením žalobu odmítl. Přípis je podle městského soudu úkonem orgánu veřejné správy, který však není správním rozhodnutím.

Proti tomuto usnesení městského soudu podal žalobce (dále též „stěžovatel") **kasační stížnost k Nejvyššímu správnímu soudu**, jíž se domáhal jeho zrušení a vrácení věci městskému soudu k dalšímu řízení.

[48] Nález Nejvyššího správního soudu ze dne 21.7.2020, 4 Azs 246/2020-27. Dostupné z: https://www.zakonyprolidi.cz/judikat/nsscr/4-azs-246-2020-27

Nejvyšší správní soud přezkoumal napadené usnesení, přitom neshledal vady uvedené, k nimž by musel přihlédnout z úřední povinnosti (např. nepřezkoumatelnost), a že v řízení bylo možno pokračovat. Nejvyšší správní soud ve věci vydal Rozsudek ze dne 18.11.2020, č.j. 4 Azs 246/2020-27. V tomto rozsudku došel Nejvyšší správní soud k následujícím závěrům a konstatováním:
V posuzované věci podal stěžovatel žádost o poskytnutí informace o zpracovávaných osobních údajích, které se ho týkaly. Právo na přístup k osobním údajům upravují ustanovení § 28 a § 30 zákona o zpracování osobních údajů. Pro účely odůvodnění rozsudku Nejvyšší správní soud citoval výše zmíněná ustanovení zákona.

Nejvyšší správní soud, po citaci ustanovení, které se týkají vyřizování žádosti, citoval formální znaky správního rozhodnutí, jsou definovány v komentáři ke správnímu řádu takto:
"Formálními znaky jsou:

- předepsaná formalizovaná podoba úkonu, který obvykle obsahuje výrok a odůvodnění;
- skutečnost, že úkon je vydáván v rámci formalizovaného postupu, byť nemusí jít o řízení ve smyslu správního řádu či daňového řádu;
- o průběhu a výsledku postupu je pořizována dokumentace,
- výsledný úkon je oznamován účastníkům řízení"

„Nejvyšší správní soud došel k závěru, že úkon spravujícího orgánu učiněný vůči subjektu údajů podle § 30 odst. 4 zákona o zpracování osobních údajů přitom všechny tyto čtyři základní podmínky neboli formální znaky rozhodnutí podle § 65 odst. 1 soudní řád správní, splňuje.“[49]

Proto není možné souhlasit se závěrem městského soudu, že žalobou napadený úkon není způsobilý zasáhnout do práv stěžovatele. Písemná informace učiněná podle § 30 odst. 4 zákona o zpracování osobních údajů je totiž ve své podstatě **zamítavým rozhodnutím** o žádosti o přístup k osobním údajům. Je evidentní, že kdyby správní orgán takové žádosti

[49] Nález Nejvyššího správního soudu ze dne 21.7.2020, 4 Azs 246/2020-27. Dostupné z: https://www.zakonyprolidi.cz/judikat/nsscr/4-azs-246-2020-27

vyhověl, stěžovatel by byl s tímto výsledkem plně spokojen a neměl by žádný důvod toto rozhodnutí napadat správní žalobou.

„Tímto úkonem, byť není výslovně označen jako rozhodnutí a není ani konečným řešením řízení vedeného podle správního řádu, tak žalovaná autoritativně rozhodla o stěžovatelově žádosti o přístup k osobním údajům, které ve vztahu k němu zpracovává.“[50]

Nejvyšší správní soud, za použití citace zákona o ochraně osobních údajů dále konstatoval, že se žalobce nemusel obracet na Úřad pro ochranu osobních údajů se stížností, před podáním žaloby k Městskému soudu, neboť k tomu není zákonem vázán. Ust. § 30 odst. 3 zákona o ochraně osobních údajů nepovažuje stížnost podanou Úřadu za řádný opravný prostředek v rámci řízení podle ust. § 28 téhož zákona. Ze znění ust. § 54 odst. 2 zákona o zpracování (ochraně) osobních údajů je taktéž zjevné, že Úřad je "pouze" orgánem kontrolním a dozorovým, a není orgánem, který by byl způsobilý v rámci své pravomoci rozhodovat o opravných prostředcích ve vztahu k řízení o písemné informaci o vyřízení žádosti. I pokud by žalobce podal stížnost k Úřadu, rozhodnutí o této stížnosti by nemělo vliv na závaznost rozhodnutí žalované podle **§ 30 odst. 4 zákona o zpracování osobních údajů.**

Podstatné je pro tuto práci zejména konstatování Nejvyššího správního soudu : *"I když by tedy bylo z praktického hlediska vhodnější, aby proti úkonu učiněnému podle § 30 odst. 4 zákona o zpracování osobních údajů, jímž nebylo žádosti o přístup k osobním údajům zcela vyhověno, bylo možné podat řádný opravný prostředek k Úřadu pro ochranu osobních údajů, nezbývá než konstatovat, že* ***takovou možnost zákonodárce nevyužil a při transpozici nařízení GDPR do vnitrostátního právního předpisu jen vyjmenoval prostředky nápravy tohoto postupu spravujícího orgánu, aniž by je přizpůsobil příslušným institutům českého právního řádu."***[51]

[50] Nález Nejvyššího správního soudu ze dne 21.7.2020, 4 Azs 246/2020-27. Dostupné z: https://www.zakonyprolidi.cz/judikat/nsscr/4-azs-246-2020-27
[51] Nález Nejvyššího správního soudu ze dne 21.7.2020, 4 Azs 246/2020-27. Dostupné z: https://www.zakonyprolidi.cz/judikat/nsscr/4-azs-246-2020-27

Celou záležitost je tedy možné uzavřít tak, že písemná informace o vyřízení žádosti o přístup k osobním údajům poskytnutá podle § 30 odst. 4 zákona o zpracování osobních údajů, **je rozhodnutím** ve smyslu § 65 odst. 1 soudní řád správní, přičemž **stížnost či podnět k Úřadu pro ochranu osobních údaj**ů směřující proti tomuto rozhodnutí nejsou **řádnými opravnými prostředky** podle § 5 ve spojení s § 68 písm. a) soudní řád správní.

Ke stejnému závěru ostatně dospěl Nejvyšší správní soud v rozsudku ze dne 9. 8. 2018, č. j. 9 Azs 49/2018 - 50, ve vztahu k informaci o vyřízení žádosti o sdělení osobních údajů vztahujících se k osobě žadatele, která se poskytovala podle § 83 odst. 5 zákona č. 273/2008 Sb., o Policii České republiky, za obdobných podmínek jako v zákoně o zpracování osobních údajů.

Závěrem pouze doplňuji výsledek řízení o kasační stížnosti:
„Stále je tedy nutno trvat na tom, že i pouhý přípis či sdělení správního orgánu mohou být posuzovány jako rozhodnutí ve smyslu ust. § 65 odst. 1 s. ř. s. v situaci, kdy je zákonem předpokládáno vydání rozhodnutí.“ (srov. např. rozsudek ze dne 29. 1. 2015, č. j. 7 As 234/2014 - 32). I přes uvedené nedostatky žalobou napadeného úkonu správního orgánu je tak zřejmé, že se jedná o rozhodnutí podle § 65 odst. 1 s. ř. s., kterým nebylo vyhověno žádosti stěžovatele o přístup k některým jeho osobním údajům.

Z uvedených důvodů městský soud pochybil, když žalobou napadený přípis žalované ze dne 21. 5. 2020, č. j. CPR-1452-2/ČJ-2020-930320, nepovažoval za rozhodnutí ve smyslu § 65 odst. 1 s. ř. s. a žalobu proti němu odmítl pro nepřípustnost.
Napadené usnesení městského soudu je tak nezákonné a důvod kasační stížnosti uvedený v § 103 odst. 1 písm. e) s. ř. s. je naplněn.“[52]
S ohledem na všechny shora uvedené skutečnosti **Nejvyšší správní soud, podle § 110 odst. 1 soudního řádu správního, napadené usnesení zrušil a věc vrátil městskému soudu k dalšímu řízení**, v němž podle odstavce čtvrtého téhož ustanovení, bude městský soud vázán právním názorem vysloveným v tomto zrušovacím rozhodnutí. Městský soud tak bude v dalším řízení vycházet z toho, že žalobou napadený úkon žalované představuje

[52] Nález Nejvyššího správního soudu ze dne 21.7.2020, 4 Azs 246/2020-27. Dostupné z: https://www.zakonyprolidi.cz/judikat/nsscr/4-azs-246-2020-27

rozhodnutí podle § 65 odst. 1 soudní řád správní, a v rozsahu žalobních námitek jej přezkoumá.

Přestože je tento judikát primárně zaměřen na procesní stránku věci (pochybení Městského soudu v Praze), důsledky odůvodnění tohoto rozhodnutí se projeví do budoucí aplikace zákona o zpracování osobních údajů, neboť na obdobné přípisy cizinecké policie, která zpracovává osobní údaje **ve veřejném zájmu**, bude nahlíženo jako na rozhodnutí, a tato pak budou muset splňovat náležitosti rozhodnutí, čímž se dále prohloubí ochrana osobních údajů – základní smysl zákona č. 110/2019 a Nařízení GDPR.

6. Výsledky a diskuse

Autorka této práce, po analýze zákona o zpracování osobních údajů a nařízení GDPR, považuje za problematickou provázanost definic pojmů mezi těmito předpisy. Autorka je přesvědčena, že by pro ochranu osobních údajů v ČR bylo přínosem, pokud by náš zákon č. 110/2019 Sb., o zpracování osobních údajů, obsahoval přímou a jasnou definici pojmu **„osobní údaj", tak jak je tomu v Nařízení GDPR.**

Chybějící definice tohoto pojmu v „našem" zákoně nijak nenapomáhá ochraně osobních údajů, neboť ta část obyvatel ČR, kteří nejsou právníky, nebo nemají právní vzdělání, bude mít potíže dohledat, co přesně je osobním údajem, neboť málokdo si je vědom principu **přímé použitelnosti** nařízení Evropského parlamentu a Rady EU (vyplývající z kauzy Van Gend en Loos, Rozsudek Soudního dvora EU ve věci 26/62 ze dne 5.2.1963). I pokud by běžný občan dohledal, že se na definici má podívat do nařízení GDPR, čeká ho nejdříve 173 odrážek recitálů, proč bylo GDPR přijato a co se jím sleduje, a až následně se dostane k samotným článkům nařízení. Nelze také odhlédnout od skutečnosti, že pojem „subjekt údajů" je v GDPR používán jako legislativní zkratka s trochu jiným významem, než jak je definován ust. § 3 zákona o zpracování osobních údajů.

Autorka shledává toto jako nedostatek zákona, který je z výše uvedených důvodů pro občany špatně čitelný a nedostatečně transparentní. Ideálním řešením by byl změna zákona, kdy by definice uvedená v čl. 4 odst. 1 GDPR byla zakomponována do našeho zákona jako samostatné ustanovení, ideálně před současné ust. § 3, jež obsahuje definici subjektu údajů. Následující ustanovení by pak měla nové číslo paragrafu o jednotku vyšší.

Dalším nedostatkem právního řádu ČR je absence konkrétní legislativy k užití dronů ve veřejném zájmu. Přestože se ve své podstatě nasazení dronu liší od kamerového systému ve městě jen tím, že dron je mobilní, problematika jeho využití by měla být šíře upravena. Autorka práce má za to, že nasazení dronů ve veřejném zájmu by mělo být validováno minimálně nařízením vlády k provedení ust. § 76 zákona č. 273/2008 Sb., o Policii ČR, aby v budoucnu nedošlo k podobné situaci jako ve Francii, viz kapitola 5 této práce.

Dále autorka práce považuje za nadmíru důležité, aby zákonodárce (potažmo příslušné správní orgány) reflektoval judikát Nejvyššího správního soudu, který je rozveden v předchozím bodu 5.3 této práce, neboť označení přípisu o (ne)poskytnutí zpracovávané

informace ve vztahu k subjektu údajů bude potřebovat minimálně změnu metodiky v chodu správních orgánů, kdy tyto orgány budou muset k podobným přípisům začít přistupovat jako k rozhodnutím ve smyslu správního řádu a bude možné proti nim podávat opravné prostředky.

7. Závěr

Autorka práce po analýze zákona č. 110/2019 Sb., o zpracování osobních údajů, dochází k závěru, že tento zákon je ve své podstatě skutečně „pouze adaptačním“ předpisem, přičemž velký význam pro společnost má zejména z důvodu, že ustavuje a upravuje (v návaznosti na předchozí předpis) chod Úřadu pro ochranu osobních údajů a dále spravujících orgánů. To však nic nemění na skutečnosti, že primárním předpisem pro ochranu osobních údajů (a způsoby jejich zpracování) je Nařízení GDPR. **Celkové znění zákona o zpracování osobních údajů se zdá být přespříliš zaměřené na ochranu veřejných zájmů, a nikoliv na ochranu zájmů soukromých, přestože úvodní ustanovení říkají opak.**

V průběhu práce byly zjištěny drobné nedostatky výše uvedeného zákona, jeden vyplývá čistě ze subjektivního názoru autorky na potřebu exaktnosti definic v předpisech, druhý pak z judikatury.

Autorka práce se domnívá, že není ku prospěchu věci celková právní roztříštěnost ochrany osobních údajů, kdy soukromí osob je poskytována (zaručována) ochrana občanským zákoníkem, zaměstnancům a zaměstnavatelům se věnuje několik ustanovení zákoníku práce a to vše je zaštítěno shora Nařízením GDPR a zákonem o zpracování osobních údajů. Bohužel, ke zpracování osobních údajů dochází neustále a při nespočetném množství činností, ať už se jedná o pracovní, úřední nebo soukromý život fyzické osoby. Jednotný předpis, který by se věnoval ochraně osobních údajů komplexněji než GDPR, asi ani není možné vytvořit.

Naopak kladně shledává autorka možnosti prolomení hranice ochrany osobních údajů ve veřejném zájmu, kdy došla k závěru, že orgány činné v trestním řízení (a ostatní orgány působící ve veřejném zájmu), mají dostatečné právní i technologické prostředky pro výkon svých funkcí. Jediným nedostatkem, co se těchto prostředků týká, je nedostatečná legislativní úprava pro užívání bezpilotních letounů - dronů, opatřených kamerovým systémem, neboť právě široké možnosti této relativně nové technologie si zcela jistě žádají regulaci právním předpisem, aby bylo zabráněno zneužití. Z dostupných zdrojů je zjevné,

že Policie ČR již bezpilotní letouny užívá pro výkon své činnosti, avšak právě zmíněná regulace použití je teprve otázkou budoucnosti, na kterou by se měl zákonodárce zaměřit.

8. Seznam použitých zdrojů

8.1. Literatura

BARTOŇ, Michal a kol. Základní práva. Praha: Leges, 2016. 608 s. ISBN 978-80-7502-128-1.

ČAPEK, Jan. Evropský soud a Evropská komise pro lidská práva: Přehled judikatury a nejzávaznějších případů. Vzory podání. 1. vydání. Praha: Linde, 1995. 642 s. ISBN 80-85647-64-8.

GERLOCH, Aleš. Veřejný zájem. In: HENDRYCH, Dušan a kol. Právnický slovník. 3., podstatně rozš. vyd. Praha: C.H. Beck, 2009, 1459 str., ISBN 9788074000591 s. 1236.

HAVLÍČEK, Aleš. Lidská a přirozená práva v dějinách. Ústí nad Labem: Universita Jana Evangelisty Purkyně, Fakulta filosofická, 2014. 236 s. ISBN 978-80-7414-620-6.

HENDRYCH, Dušan a kol. Právnický slovník. 3., podstatně rozš. vyd. Praha: C.H. Beck, 2009, 1459 s. ISBN 9788074000591.

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

KNAP, Karel, ŠVESTKA, Jiří, JEHLIČKA, Oldřich, PAVLÍK, Pavel, PLECITÝ, Vladimír. Ochrana osobnosti podle občanského práva. 4. vyd. Praha: Linde, 2004. 435 s. ISBN 80-7201-484-6.

KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012. 536 s. ISBN 978-80-7179-226-0.

LIPPMANN, Walter. Essays in the public philosophy. Boston, Toronto. Little, Brown and Company 1955. 42 s.

MOLEK, Pavel. Základní práva. Svazek první., Důstojnost. Praha. Wolters Kluwer, Lidská práva, 2017. 549 s. ISBN 978-80-7552-167-5.

NONNEMANN, František, KUČEROVÁ, Alena a kol. Zákon o ochraně osobních údajů. Praha: C. H. Beck, 2012. 50 s. (§ 4 písm. a))

NULÍČEK, Michal, DONÁT, Josef, LICHNOVSKÝ, Bohuslav, NONNEMANN, František, HABERTA, Petr, KAŠPÁRKOVÁ, Kateřina. Zákon o zpracování osobních údajů. Praha. Wolters Kluwer ČR, 2019. 212 s. ISBN 978-80-7598-467-8.

ONDŘEJOVSKÁ, Eva. Ochrana osobnosti v common low a českém právu. Praha: Leges, Teoretik, 2016. 256 s. ISBN 978-80-7502-164-9.

VLACHOVÁ, Barbora, MAISNER, Martin. Zákon o zpracování osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2019, 168 s. ISBN 978-80-7400-760-6.

VOJÁČEK, Ladislav, SCHELLE, Karel. České právní dějiny do roku 1945. 1. vydání. Ostrava: KEY Publisching, 2007. 218 s. ISBN 987-80-87071-20-5.

PAVLÍČEK, Václav a kol. Ústavní právo a státověda, II. Díl. Ústavní právo České republiky. 3. vydání. Praha: Leges, 2020. 1160 s. ISBN 978-80-7502-468-8.

WAGNEROVÁ, Eliška a kol. Listina základních práv a svobod: komentář. Praha: Wolters Kluwer, 2012. 906 s. ISBN 978-80-7357-750-6.

8.2. Legislativa

Ústavní zákon číslo 1/1993 Sb., ze dne 16. 12. 1992, Ústava České republiky, ve znění pozdějších předpisů (ústava).

Ústavní zákon číslo 2/1993 Sb., ze dne 16. 12. 1992, Listina základních práv a svobod, ve znění pozdějších předpisů (listina).

Ústavní zákon č. 110/1998 Sb., ze dne 22. 4. 1998, o bezpečnosti České republiky.

Ústavní zákon číslo 293/1920 Sb., ze dne 9. 4. 1920, o ochraně svobody osobní, domovní a tajemství listovního (podle §§ 107, 112 a 116 ústavní listiny).

Zákon č. 40/1964 Sb., ze dne 26. 2. 1964, občanský zákoník.

Zákon č. 40/2009 Sb., ze dne 8. 1. 2009, trestní zákoník, ve znění pozdějších předpisů.

Zákon č. 89/2012 Sb., ze dne 3. 2. 2012, občanský zákoník, ve znění pozdějších předpisů.

Zákon č. 101/2000 Sb., ze dne 4. 4. 2000, o ochraně osobních údajů, ve znění pozdějších předpisů.

Zákon č. 106/1999 Sb., ze dne 11. 5. 1999, o svobodném přístupu k informacím.

Zákon č. 110/2019 Sb., ze dne 12. 3. 2019, o zpracování osobních údajů, ve znění pozdějších předpisů.

Zákon č. 128/2000 Sb., ze dne 12. 4. 2000, o obcích.

Zákon č. 141/1961 Sb., ze dne 29. 11. 1961, o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

Zákon č. 153/1994 Sb., ze dne 7. 7. 1994, o zpravodajských službách České republiky.

Zákon č. 234/2014 Sb., ze dne 1.10. 2014, o státní službě.

Zákon č. 250/2016 Sb., ze dne 12. 7. 2016, o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů.

Zákon č. 251/2005 Sb., ze dne 3. 5. 2005, o inspekci práce, ve znění pozdějších předpisů.

Zákon č. 255/2012 Sb., ze dne 14. 6. 2012, o kontrole, ve znění pozdějších předpisů.

Zákon č. 256/1992 Sb., ze dne 29. 4. 1992, o ochraně osobních údajů v informačních systémech.

Zákon č. 262/2006 Sb., ze dne 21. 4. 2006, zákoník práce, ve znění pozdějších předpisů.

Zákon č. 273/2008 Sb., ze dne 17. 7. 2008, o Policii České republiky, ve znění pozdějších předpisů.

Zákon č. 289/2005 Sb., ze dne 16. 6. 2005, o Vojenském zpravodajství.

Zákon č. 293/1920 Sb., ze dne 9. 4. 1920, o ochraně svobody osobní, domovní a tajemství listovního.

Zákon č. 300/1920 Sb., ze dne 14. 4. 1920, o mimořádných opatřeních.

Zákon č. 412/2005 Sb., ze dne 21. 9. 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Zákon č. 500/2004 Sb., ze dne 24. 6. 2004, správní řád.

Zákon č. 553/1991 Sb., ze dne 6. 12. 1991, o obecní policii, ve znění pozdějších předpisů.

Směrnice Evropského parlamentu a Rady 95/46/ES, ze dne 24. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

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

(GDPR – General Data Protection Regulation)

Nařízení republiky Československé č. 636/1920 Sb., ze dne 12. 12. 1920, kterým se zavádějí mimořádná opatření.

8.3. Internetové zdroje

CARR, Nancy K., *Programmed to Protect and Serve: The Dawn of Drones and Robots in Law Enforcement,* 86 JOURNAL OF AIR L. & COM. 183 (2021), str. 201, dostupné [online] https://scholar.smu.edu/cgi/viewcontent.cgi?article=4169&context=jalc

Informace o provozování kamerových systémů. Ministerstvo vnitra, dostupné [online]: http://www.mvcr.cz/clanek/informace-o-provozovani-kamerovych-systemu.aspx Poslední přístup dne 6.2. 2021

JOUZA, Ladislav. Právní ochrana elektronické pošty zaměstnanců, [online] dostupné z: https://www.epravo.cz/top/clanky/pravni-ochrana-elektronicke-posty-zamestnancu-112612.html

KONÍČEK, Tomáš. Městské kamerové dohlížecí systémy v praxi obcí a měst v České republice, dostupné [online] http://denik.obce.cz/clanek.asp?id=6737369

kpt. Mgr. Lenka Sikorová, mluvčí PČR, dostupné [online] https://www.policie.cz/clanek/vybaveni-letecke-sluzby-pcr-novymi-drony.aspx

MATZNER, Jiří. Může zaměstnavatel sledovat vaší aktivitu na internetu nebo pracovní emaily? [online] dostupné z: https://digibiz.cz/muze-zamestnavatel-sledovat-vasi-aktivitu-na-internetu-nebo-pracovni-emaily/

Metodika provozování kamerových systémů vypracovaná ÚOOÚ, dostupné [online] http://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf

Nález Nejvyššího správního soudu ze dne 21.7.2020, 4 Azs 246/2020-27. Dostupné z: https://www.zakonyprolidi.cz/judikat/nsscr/4-azs-246-2020-27

Rozhodnutí Státní rady Francie ze dne 18.5.2020, Nos. 440442, 440445, dostupné [online] https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones

Rozsudek Nejvyššího správního soudu ze dne 23.10.2003, č.j. 2 As 11/2003-164, [232/2004 Sb. NSS]

Stanovisko veřejné ochránkyně práv ze dne 30.10.2019, č.j. KVOP-47586/2019, dostupné [online] https://eso.ochrance.cz/Nalezene/Edit/7540

Úřad pro kontrolu osobních údajů. Dostupné z [online]: https://www.uoou.cz/pusobnost/ds 1269/archiv=0&p1=1059.

Úřad pro kontrolu osobních údajů, dostupné [online] http://www.itpoint.cz/uoou/

Úřad pro civilní letectví, Ministerstvo dopravy České Republiky, Letecký předpis – Pravidla létání L2, č.j.: 153/2014-220, dostupné [online] https://aim.rlp.cz/predpisy/predpisy/index.htm

Veřejný zájem, dostupné [online] https://iuridictum.pecina.cz/w/Veřejný_zájem

https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679#d1e1396-1-1

9. Přílohy

Souhlas se zpracováním osobních údajů

Souhlas se zpracováním osobních údajů

Společenství vlastníků jednotek v budově 777-779, Brechtova ul., Praha 4

Prohlašuji, že jsem byl seznámen s následujícími skutečnostmi týkající se provozování kamerového systému se záznamem ve společných prostorách objektu Brechtova 777,778 a 779, Praha 4 provozovaného Společenstvím vlastníků jednotek v budově 777-779, Brechtova ul., Praha 4 (dále jen SVJ):

1) Účelem provozovaní kamerového systému se záznamem je ochrana života a zdraví obyvatel domu a jejich návštěv, ochrany proti vandalismu, krádežím, vloupáním a zamezení vstupu nežádoucích osob do společných částí domu.
2) Kamerový systém tvoří kamery monitorující hlavní přístupové chodby v domě a nahrávací zařízení umístěné v kanceláři Výboru SVJ.
3) Záznamy jsou uchovávány po dobu 7 dní.
4) Správcem osobních údajů je Výbor SVJ.
5) Bližší informace lze získat na webových stránkách SVJ www.brechtova.cz

Souhlasím se zpracováním osobních údajů dle zákona č. 101/2000 Sb., zákon o ochraně osobních údajů:

Osoby užívající byt č.:	č. popisné:	
Příjmení a jméno*	Datum narození	Datum a podpis

**Je vyžadováno vyjádření všech byt obývajících osob (nebo jejich zákonných zástupců)*