

Univerzita Karlova

Právnická fakulta

Jakub Lejsek

Ochrana osobních údajů a pracovněprávní vztahy

Diplomová práce

Vedoucí diplomové práce: JUDr. Jakub Morávek, Ph.D.

Katedra pracovního práva a práva sociálního zabezpečení

Datum vypracování práce (uzavření rukopisu): 20. 8. 2017

Prohlašuji, že předloženou diplomovou práci jsem vypracoval samostatně a že všechny použité zdroje byly řádně uvedeny. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Jakub Lejsek

Poděkování

Děkuji svému vedoucímu práce, JUDr. Jakubu Morávkovi, Ph.D., za ochotu vést mou diplomovou práci, trpělivý přístup a za cenné rady, které mi při psaní práce poskytoval.

Obsah

Úvod	1
1. Právo na soukromí.....	5
2. Právní úprava ochrany osobních údajů a soukromí.....	9
2.1 Organizace spojených národů.....	9
2.2 Rada Evropy.....	12
2.3 Evropská unie.....	14
2.4 Česká republika.....	20
2.4.1 Ústavní pořádek České republiky.....	21
2.4.2 Občanský zákoník.....	23
2.4.3 Zákon o ochraně osobních údajů	24
2.4.4 Zákoník práce	25
2.4.5 Trestní zákoník a ZTOPO	27
3. Základní pojmosloví ochrany osobních údajů	29
3.1 Osobní údaj	29
3.2 Citlivý osobní údaj	32
3.3 Anonymní údaj	36
3.4 Subjekt údajů.....	37
3.5 Zpracování osobních údajů	40
3.6 Správce	41
3.7 Zpracovatel.....	43
3.8 Souhlas subjektu údajů	45
4. Povinnosti zaměstnavatele a práva zaměstnance	49
4.1 Povinnosti správce osobních údajů a práva subjektu údajů	49
4.2 Obecné nařízení a změny v právech a povinnostech stran.....	53
5. Zpracování osobních údajů v jednotlivých fázích pracovního poměru...	60

5.1	Zpracování osobních údajů před vznikem pracovního poměru	60
5.2	Zpracování osobních údajů v průběhu pracovního poměru	64
5.3	Zpracování osobních údajů po skončení pracovního poměru	68
6.	Sledování zaměstnanců	69
6.1	Sledování aktivity zaměstnanců na internetu	73
6.2	Monitorování e-mailové korespondence.....	77
6.3	Monitorování služebních telefonů.....	80
6.4	Kontrola služebních automobilů	81
6.5	Kamerové systémy.....	82
	Závěr.....	86
	Seznam zkratk	89
	Seznam zdrojů	91
	Resumé	101
	Summary	102
	Klíčová slova.....	104
	Keywords	104
	Název práce v anglickém jazyce.....	104

Úvod

Osobní údaje provází každého již od samotného narození až do jeho skonu. Jejich existence tvoří šlépěj života osob, bez které by osoba pro druhé někdy ani neexistovala. Ochrana osobních údajů představuje poměrně mladou právní disciplínu, která se začala dynamicky rozvíjet zejména v osmdesátých a devadesátých letech minulého století v korelaci s technologickým rozvojem a informačním „boomem“. S rozšířením technologických vymožeností a internetu prakticky do každé domácnosti ve vyspělých zemích světa a s rozkvětem sociálních sítí dochází ke zveřejňování osobních údajů velmi snadným způsobem a například fotografie, které si lidé dříve uchovávali v rodinných albech jen pro blízký okruh přátel a na památku, si mohou během několika kliknutí zobrazit nejen širší přátelé či známí, ale mnohdy také kdokoli, kdo ať už náhodně, či cíleně zavítá na daný profil.

V dnešní době mnoho osob nakládá se svými osobními údaji velmi lehkomyšlně, aniž by si uvědomovali rizika s tím spojená. Tím usnadňují pozici subjektům, pro něž takové informace představují velmi ceněnou komoditu, kterou mohou využít především v obchodním styku. Bývalá eurokomisařka Meglena Kuneva dokonce prohlásila, že *„osobní údaje jsou novou ropou internetu a nová měna digitálního světa.“*¹ Z tohoto důvodu také dochází k intenzivnímu vývoji „špiclovacích“ informačních technologií, které jsou obvykle o krok napřed než právní úprava.

„Velký bratr tě sleduje“, pomyslný citát z Orwellova románu 1984 dnes už nelze chápat jako pouhou frázi z proslulého díla, ale jako realitu dnešní společnosti a ohrožení soukromého života fyzických osob. Všudypřítomné novinové titulky či televizní zpravodajství obklopují lidi hromadnými úniky osobních údajů k nekalým účelům.

Obchodníci velmi často nabízejí osobám členství v různých klubech, které jsou navenek prezentovány jako věrnostní programy, které poskytují členům slevy či jiné výhody. Zákazník se obvykle nedozví bez toho, aby četl dlouhé a většinou pro osobu

¹ KUNEVA, MEGLENA *Keynote Speech. Roundtable on Online Data Collection, Targeting and Profiling*. Brusel dne 31. 3. 2009 Dostupné z http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm [cit. 11. 3. 2017]

bez právního vzdělání nesrozumitelné podmínky, v jakém rozsahu dochází ke zpracování osobních údajů zákazníka. Je tedy na každém zda se „upíše ďáblu“ a obdrží určitou výhodu či naopak bude střežit své soukromí.

Možná i tento fakt vede osoby, aby se zamysleli nad tím, že soukromí není jen abstraktní pojem, ale také „statek“, který jím umožní, pokud možno nerušený a klidný život. S tím také souvisí snaha omezit nežádoucí předávání či úniky osobních údajů a chránit soukromí fyzických osob. Mnohdy se ochrana soukromí dostává do střetu s jinými ústavně chráněnými zájmy, zejména ochranou vlastnictví nebo bezpečností, mezi nimiž se musí důkladně poměřovat a pečlivě zvážit jakýkoliv zásah do soukromí. Za cíl právní úpravy ochrany osobních údajů či soukromí nelze považovat zákaz či podstatné omezení zpracování osobních údajů, které by se vzhledem k dnešní době jevilo jako krok zpět a zřejmě by bylo i nemožné. Takový cíl lze tedy spatřovat v zajištění účinné ochrany osobních údajů, které by pokud možno zamezilo neoprávněným zásahům do soukromí osob či alespoň omezilo jejich kvantitu a následky těchto zásahů.

Ochranu soukromí a osobních údajů nelze striktně zařadit do určitého právního odvětví, jelikož zasahuje prakticky do každého z nich, a to jak v oborech práva veřejného, tak i v oborech práva soukromého. Jednu z nejpodstatnějších oblastí, kde dochází ke zpracování osobních údajů, představují individuální pracovněprávní vztahy, tj. vztahy vznikající při výkonu závislé práce mezi zaměstnanci a zaměstnavateli. V pracovněprávních vztazích se nelze vyhnout zpracování osobních údajů, jelikož zákonná úprava dokonce určité zpracování osobních údajů zaměstnavateli nařizuje. Cílem zaměstnanců dnes již není pouze snaha získávat prostředky pro své životní potřeby prací, ale také možnost seberealizace, kariérního růstu či budování a rozvíjení vztahů na pracovišti v rámci svých pracovních aktivit.

Zaměstnavatelé tak nutně přicházejí do styku s osobními údaji svých zaměstnanců, a to nejen v rámci pracovněprávního vztahu, ale i před jeho případným započítím v tzv. prepracovní fázi a také po jeho skončení.

Mimo případy stanovené zákonem nejeden zaměstnavatel zpracovává i jiné údaje o zaměstnancích než které je povinen, např. ke své propagaci zveřejňuje

profily svých zaměstnanců včetně fotografií na svých webových stránkách, k ochraně vlastního majetku sleduje celé své pracoviště či pomocí GPS lokalizuje ujetou vzdálenost a trasu zaměstnanec služebním automobilem. K takovému zpracování je ovšem obvykle nutný souhlas zaměstnanec. Lze však takový souhlas zaměstnanec považovat za svobodný, když vykonává pro zaměstnavatele závislou práci ve vztahu podřízenosti a podle pokynů zaměstnavatele? Na druhou stranu je nutné zdůraznit, že rozvoj a informační boom nepřináší pouze rizika, ale i mnoho výhod a usnadňuje nejen zaměstnancům výkon jejich práce.

S ohledem na to, že zvolené téma, tedy ochrana osobních údajů a pracovněprávní vztahy, představuje velmi širokou problematiku, která by si bezpochyby zasloužila rozsáhlejší pozornost, nežli zpracování v rámci diplomové práce, považuje autor za cíl této práce zejména přiblížit obecnou problematiku osobních údajů, včetně základních pojmů a následně se zaměřit na praktické aspekty zpracování osobních údajů v různých fázích pracovněprávních vztahů.

O aktuálnosti tématu hovoří i to, že tato problematika tvoří otevřenou kapitolu a i v budoucnu bude nutné neustále reagovat na nové technologie a jejich invaze a nové způsoby jak zasáhnout do soukromí. Pracovněprávní vztahy ve 21. století neslouží zaměstnancům pouze k získání prostředků pro své životní potřeby, ale také k určité seberealizaci daného zaměstnanec či k sociální interakci s dalšími jedinci. Z tohoto důvodu není možné nahlížet na zaměstnanec jako na pouhý lidský zdroj, nýbrž jako na lidskou osobnost, která má, kromě povinností, i svá práva.

Diplomová práce je systematicky členěna do 6 kapitol a metodologicky je řešena postupem od abstraktních či obecných právních pojmů, shrnutí právní úpravy v mezinárodní i národní dimenzi ke konkrétním případům zpracování osobních údajů týkající se všech fází pracovního poměru.

V první části této práce bude věnována pozornost přiblížení pojmu soukromí, v druhé kapitole bude rozebírána právní úprava ochrany soukromí a osobních údajů, a to nejen v rámci právního řádu České republiky, ale také mezinárodněprávní a regionální úprava včetně práva *sui generis*, za něž se tradičně označuje právní řád Evropské unie, z nichž národní právní úprava ve značné míře vychází. V třetí části této práce bude popsáno základní pojmosloví ochrany osobních údajů, jehož znalost

je nutná k náležitému pochopení celé problematiky. Čtvrtá část této práce bude pojednávat o povinnostech zaměstnavatele a s tím souvisejícími právy zaměstnanců.

V další části této práce bude předmětem zájmu již zpracování osobních údajů před případným uzavřením pracovního poměru, v rámci pracovního poměru, ale také po jeho skončení. A konečně v poslední části bude pozornost zaměřena na sledování zaměstnanců.

1. Právo na soukromí

Ačkoliv je pojem soukromí užíván již po velmi dlouhou dobu, tak jeho definování působí i v dnešní době značné potíže a jeho legální definici nejen v českém právním řádu není možné nalézt. Soukromí nelze chápat jako neměnnou veličinu, pod kterou si každý představí stejné hodnoty či zájmy. Definování soukromí je závislé jednak na místě a čase, ale také na národnosti, kulturních hodnotách či společenském postavení.² V minulosti bylo soukromí pojímáno zejména jako určitý prostor, do kterého nesmí nikdo bez zákonného oprávnění či svolení dotčené osoby zasahovat.³ Soukromí bylo obvykle chráněno souborem dílčích práv a samotné soukromí, jakožto samostatné právo *stricto sensu* chráněno nebylo.

Jednu z prvních teoretických definic představil Samuel Warren a Louis Brandeis ve svém dnes již kultovním článku prezentovaném v *Harvard Law Review* již v roce 1890. Tito američtí právníci chápali právo na soukromí jako „*právo na to být ponechán o samotě (right to be let alone)*“.⁴

O několik let později Brandeis takto striktní pojetí práva na soukromí rozšířil ve svém disentaním stanovisku ve věci *Olmstead v. USA*, kde pojetí práva na soukromí chápal již jako právo směřující k zachování nerušeného klidu, neporušování citů subjektu a neznepokojování ve vlastním obydlí.⁵

Ve druhé polovině minulého století nabyla ochrana soukromí na významu po neblahých zkušenostech s autoritativními a totalitními režimy, kdy se začalo prosazovat přirozeněprávní pojetí základních lidských práv, které bylo následováno zakotvením lidských práv nejen do mezinárodních smluv, ale také do ústav

² MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 58. ISBN 978-80-7478-139-1.

³ MATES, PAVEL *Ochrana osobních údajů*. Vyd. 1. Praha: Karolinum, 2002, s. 37. ISBN 80-246-0469-8.

⁴ WARREN, SAMUEL; BRANDEIS, LOUIS, *The Right to Privacy*. in *Harvard Law Review* 890 Vol. IV, 193

⁵ MATES, Pavel *Ochrana soukromí ve správním právu*. 2. aktualizované a podstatně přepracované vyd. Praha: Linde, 2006, s. 11. ISBN 80-7201-589-3.

jednotlivých států, v nichž dochází k pouhé deklaraci těchto práv, jelikož základní lidská práva existují bez ohledu na jejich zakotvení v právních předpisech.

Soukromí mimo jiné umožňuje člověku oprostít se od svých sociálních rolí, na nic si nehrát, čímž dochází k emočnímu uvolnění jedince s možností vyjadřovat své pocity, úzkosti, názory či dokonce možnost porušovat sociální konvence a společenskou etiketu.⁶

Právo na soukromí obsahuje jak pozitivní složku, která spočívá v možnosti člověka zpřístupňovat druhým své soukromé údaje, tak také složku negativní. Tu lze naopak charakterizovat jako právo vzepřít se proti neoprávněným zásahům do svého soukromí ze strany jiných osob.⁷

Právo na soukromí nelze považovat za právo absolutní, a tudíž lze za určitých podmínek přistoupit i k jeho omezení. Podle Ústavního soudu lze k omezení přistoupit „*za účelem ochrany základních práv jiných osob, anebo za účelem ochrany veřejného zájmu, který je v podobě principu či hodnoty obsažen v ústavním pořádku.*“⁸

Vzhledem k tomu, že ochrana soukromí představuje velmi důležitou oblast zpracování osobních údajů, tak se k pojmu soukromí vyjádřil i UOOU ve stanovisku č. 6/2009, kde chápe soukromí jako „*osobní, intimní sféru člověka v jeho integritě, která zahrnuje všechny projevy osobnosti konkrétního a jedinečného lidského tvora.*“⁹

Ačkoliv právo na soukromí a ochrana osobních údajů spolu velmi úzce souvisí a vzájemně se prolínají, tak se nejedná o synonyma. Právo na ochranu osobních

⁶ FIALOVÁ, EVA *Bezkontaktní čipy a ochrana soukromí*. Praha: Leges 2016, s.45. ISBN 978-80-7502-150-2.

⁷ Usnesení Ústavního soudu ze dne 1. března 2000, sp. zn. II. ÚS 517/99

⁸ Nález Ústavního soudu ze dne 18. prosince 2006, sp. zn. I. ÚS 321/06

⁹ srov. UOOU Stanovisko č. 6/2009 - *Ochrana soukromí při zpracování osobních údajů*. Dostupné z https://www.uouu.cz/files/stanovisko_2009_6.pdf [cit. 27. 3. 2017]

údajů se týká pouze informací, které lze podřadit pod pojem osobní údaj. V opačném případě takové informace nepožívají ochrany práva na ochranu osobních údajů.¹⁰

Jedním z prvků práva na soukromí je i soukromí zaměstnance na pracovišti. Názor, že pracoviště zaměstnanci neslouží k realizaci svého soukromého života či k navazování mezilidských vztahů, nýbrž výhradně k plnění předmětu pracovněprávního vztahu, tedy ke konkrétnímu výkonu práce, již v dnešní době neobstojí. Zaměstnavatelé by měli brát v potaz, že poměrně mnoho činností běžně vykonávaných v rámci pracovněprávního vztahu může souviset s ochranou soukromí či osobních údajů zaměstnance a z toho důvodu by tuto problematiku neměli chápat jen jako vedlejší či okrajovou.

Zaměstnanci mají dle článku 28 Listiny základních práv a svobod právo na uspokojivé pracovní podmínky. Takové podmínky nelze zaměřovat pouze s přiměřenou teplotou, vlhkostí, prašností, hlukem či osvětlením na pracovišti, avšak je nutné zohlednit i sociální interakci mezi zaměstnanci, rozvoj zaměstnance a ochranu jeho soukromí.¹¹

K definici pojmu soukromí přispělo také hojně citované rozhodnutí Evropského soudu pro lidská práva ve věci Niemietz v. Německo, kde soud zahrnul do pojmu soukromí člověka i jeho právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi. Dle názoru soudu má většina zaměstnanců během svých pracovních aktivit značnou a možná i největší příležitost navázat a rozvíjet vztahy s vnějším okolím, a to je právě důvodem, aby právo na respektování soukromého života zahrnovalo i respektování soukromí v zaměstnání.¹²

Ústavní soud se k tomuto obdobně vyjádřil ve svém nálezu ze dne 22. 3. 2011, sp. zn. Pl. 24/10, kde vykládá soukromí následovně: „*Primární funkcí práva na respekt k soukromému životu je zajistit prostor pro rozvoj a seberealizaci individuální osobnosti. Vedle tradičního vymezení soukromí v jeho prostorové dimenzi (ochrana*

¹⁰ FIALOVÁ, EVA *Bezkontaktní čipy a ochrana soukromí*. Praha: Leges 2016, s.43. ISBN 978-80-7502-150-2.

¹¹ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 66. ISBN 978-80-7478-139-1.

¹² Niemietz v. Německo z roku 1992 stížnost č. 13710/88

obydlí v širším slova smyslu) a v souvislosti s autonomní existencí a veřejnou mocí nerušenou tvorbou sociálních vztahů (v manželství, v rodině, ve společnosti), právo na respekt k soukromému životu zahrnuje i garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém. Jinými slovy, právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům.“

Na výše uvedený rozsudek ESLP navázal i Nejvyšší správní soud ve svém rozhodnutí, kdy nepřipustil jako důkazní prostředek audiovizuální záznam pořízený utajeně orgánem veřejné moci uvnitř vozidla taxikáře s odůvodněním, že došlo k zásahu do soukromého života taxikáře, jelikož taxikář tráví ve svém vozidle převážnou část svého pracovního dne a během výkonu své práce navazuje a rozvíjí kontakty se svými klienty. V opačném případě by bylo velmi problematické rozlišit osobní projevy taxikáře od jeho pracovní činnosti.¹³

Jakub Morávek při pojetí soukromí na pracovišti dochází k obecnému pravidlu, a to „*nečiň jinému to, co nechceš, aby on činil tobě*“.¹⁴ S tímto pravidlem nelze než souhlasit, ovšem i tak se s ním nelze plně uspokojit, jelikož každá osoba vnímá soukromí jiným způsobem a mnoho zaměstnanců nikdy nevystupovalo v roli zaměstnavatele a opačně. Z tohoto důvodu může být v daném případě pro jakoukoliv ze stran někdy obtížné odhadnout závažnost či míru konkrétního zásahu do soukromí jedince.

¹³ Rozhodnutí Nejvyššího správního soudu ze dne 5. listopadu 2009, sp. zn. 1 Afs 60/2009 - 119

¹⁴ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 67. ISBN 978-80-7478-139-1.

2. Právní úprava ochrany osobních údajů a soukromí

Předmětem této kapitoly je přiblížit právní úpravu ochrany osobních údajů a soukromí jak na úrovni mezinárodní a regionální, tak také na národní úrovni. Vzhledem k přirozeněprávní povaze práva na ochranu soukromí je možné toto právo nalézt v mnoha mezinárodních smlouvách či jiných závazných dokumentech mezinárodního práva, z nichž lze v oblasti lidských práv a svobod označit za průkopníka Všeobecnou deklaraci lidských práv.

Dle článku 10 Ústavy „Vyhlášené mezinárodní smlouvy, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána, jsou součástí právního řádu“ a v případě rozporu se zákonem se použije právě mezinárodní smlouva. S ohledem na to, že v globalizovaném světě dochází velmi často k předávání osobních údajů do zahraničí, tak tuto problematiku nelze řešit pouze na národní úrovni.¹⁵ Také z tohoto důvodu je velmi důležité uvést mezinárodněprávní úpravu, která byla rovněž inspirací pro tvůrce ústav či katalogů základních lidských práv v moderních právních rádech.

Mezinárodní prameny vznikaly také na regionální úrovni, a to především na poli Rady Evropy a Evropské unie. Vzhledem ke členství České republiky v Evropské unii je nutné vzít v potaz také právní řád tohoto společenství, z něž zákon o ochraně osobních údajů vychází.

2.1 Organizace spojených národů

K zakotvení lidských práv jako práv přirozeněprávních došlo v roce 1945 Chartou OSN, která prohlásila lidskou důstojnost a základní lidská práva za cíl OSN.^{16 17} Jelikož jednotlivá ustanovení Charty OSN byla jen velmi obecná, tak došlo k jejich konkretizaci ve Všeobecné deklaraci lidských práv, která byla schválena Valným shromážděním OSN dne 10. 12. 1948. Tato deklarace je „společným cílem

¹⁵ JANEČKOVÁ, EVA, BARTÍK, VÁCLAV *Ochrana osobních údajů v pracovním právu (Otázky a odpovědi)*. Praha: Wolters Kluwer, 2016, s. 11. ISBN 978-80-7552-145-3.

¹⁶ POTOČNÝ, MIROSLAV, ONDŘEJ, JAN *Mezinárodní právo veřejné – Zvláštní část*. 6. doplněné a rozšířené vydání. Praha: C.H. Beck, 2011, s. 98. ISBN 978-80-7400-398-1.

¹⁷ pozn. Charta sice vstoupila v platnost 25. 10. 1945, ovšem OSN prakticky zahájila činnost až dne 20. 1. 1946 prvním zasedáním Valného shromáždění

pro všechny národy a státy“ a hlásí se ke svobodě a rovnosti mezi lidmi s velkým důrazem na lidskou důstojnost. Ochrana soukromého života je upravena v článku 12, který stanoví: „Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst.“ Druhou větu tvoří zákonná garance ochrany každého, kdo takovým zásahům či útokům čelil nebo stále čelí.

Z pracovněprávního pohledu má relevanci pro zaměstnavatele zejména právo chránit svůj majetek dle článku 17 a pro zaměstnance článek 23 odst. 1, který mimo práva na práci, zmiňuje také právo zaměstnance na spravedlivé a uspokojivé pracovní podmínky. Nelze opomenout fakt, že Všeobecná deklarace měla pouze doporučující povahu a její ustanovení nebyla právně závazná, ovšem pravidla v ní obsažená se postupně objevovala v ústavách mnohých států a lidskoprávních smlouvách, čímž se tato pravidla přeměnila v pravidla závazná.¹⁸ Mimo to lze také podotknout, že v dnešní době lze již Deklaraci považovat za obyčejové pravidlo, které v mezinárodním právu veřejném tvoří jeden z pramenů práva.¹⁹

O osmnáct let později přijalo Valné shromáždění OSN dvě, již závazné, mezinárodní úmluvy, a to Mezinárodní pakt o občanských a politických právech a Mezinárodní pakt o hospodářských, sociálních a kulturních právech. Dosažení konsenzu vzhledem k závaznosti těchto dokumentů a odlišným představám zejména západních a socialistických států bylo velmi problematické, a tak výsledná podoba představuje kompromis, který je považován za „*minimální obecný standard lidských práv*.“²⁰

Mezinárodní pakt o občanských a politických právech navazuje na přirozenou důstojnost lidské bytosti a všeobecnou úctu k lidským právům a svobodám obsaženým ve Všeobecné deklaraci lidských práv a na zásady vyhlášené v Chartě OSN. Z hlediska rozebírané problematiky se nejpodstatněji jeví článek 17, který

¹⁸ POTOČNÝ, MIROSLAV, ONDŘEJ, JAN *Mezinárodní právo veřejné – Zvláštní část*. 6. doplněné a rozšířené vydání. Praha: C.H. Beck, 2011, s. 98. ISBN 978-80-7400-398-1.

¹⁹ k tomuto srov. ČEPELKA, ČESTMÍR, ŠTURMA, PAVEL *Mezinárodní právo veřejné*. 1. vydání. Praha: C.H. Beck, 2008, s. 97 a násl. ISBN 978-80-7179-728-9.

²⁰ POTOČNÝ, MIROSLAV, ONDŘEJ, JAN *Mezinárodní právo veřejné – Zvláštní část*. 6. doplněné a rozšířené vydání. Praha: C.H. Beck, 2011, s. 100. ISBN 978-80-7400-398-1.

opisuje článek 12 Všeobecné deklaráce. Důležitost zopakování tohoto článku vychází z kontextu celého paktu, který v článku 2 zavazuje smluvní státy k respektování obsažených práv a zavazuje je, aby uvedly do souladu národní předpisy způsobem odpovídajícím tomuto Paktu.

To ostatně platí i o druhém paktu, kterým je Mezinárodní pakt o hospodářských, sociálních a kulturních právech. Na rozdíl od předchozího paktu, který obsahuje stejnou formulaci zákazu zasahování do soukromého života jako Deklarace, tak v tomto paktu v článku 7 nalezneme právo každého člověka na spravedlivé a uspokojivé pracovní podmínky rozšířené o výčet prvků, které naplňují tento pojem. Nutno podotknout, že se jedná pouze o demonstrativní výčet, a tak se v průběhu doby v korelaci s rozvojem společnosti a technologií jedná o proměnnou kategorii, do níž lze v dnešní době jistě zařadit i ochranu soukromí zaměstnance na pracovišti.²¹ Článek 7 se zmiňuje o právu na spravedlivé a uspokojivé pracovní podmínky v oblasti odměňování, bezpečných a zdravotně nezávadných pracovních podmínek, stejných příležitostí v zaměstnání či o odpočinku a rozumné pracovní době.

V rámci této podkapitoly nelze nezmínit Mezinárodní organizaci práce (*International Labour Organization*),²² která patří mezi nejvýznamnější odborné organizace přidružené k OSN.²³ Tato organizace přijímá, jak lze dovodit z jejího názvu, mezinárodní úmluvy, doporučení a rezoluce v oblasti pracovního a také sociálního zákonodárství a ostatních souvisejících otázek. Z hlediska tématu diplomové práce je nejdůležitějším aktem z „dílny“ Mezinárodní organizace práce její Kodex ochrany osobních údajů zaměstnanců, jehož cílem je zajištění ochrany osobních údajů, soukromí a důstojnosti zaměstnanců.²⁴ Účelem kodexu je

²¹ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 92. ISBN 978-80-7478-139-1.

²² pozn. Mezinárodní organizace práce byla založena již v roce 1919 v rámci Pařížské mírové konference

²³ ŠTANGOVÁ, VĚRA in BĚLINA, MIROSLAV a kol. *Pracovní Právo*. 6. Doplněné a podstatně přepracované vydání. Praha: C.H. Beck, 2014, s. 39. ISBN 978-80-7400-283-0.

²⁴ International Labour Organization *Code of practice on the protection of workers' personal data*. Dostupné z http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf [cit. 13. 3. 2017]

poskytnout vodítko k ochraně osobních údajů zaměstnanců a na rozdíl od některých jiných dokumentů Mezinárodní organizace práce není právně závazným.²⁵

2.2 Rada Evropy

Rada Evropy představuje nejstarší politickou evropskou organizaci, jejíž hlavním cílem je dosažení jednoty mezi členskými státy za účelem zabezpečení realizace společných ideálů a zásad. Rada Evropy již přijala velký počet mezinárodních smluv, dohod či protokolů, z nichž bezpochyby nejvýraznějším počinem je Úmluva o ochraně lidských práv a svobod z roku 1950 („**Evropská úmluva**“).

Evropská úmluva poskytuje ochranu lidským právům prostřednictvím Evropského soudu pro lidská práva, který sídlí ve Štrasburku. Tento soudní orgán má pravomoc v mezistátních případech a také rozhoduje o individuálních stížnostech proti smluvním státům podaných fyzickou osobou, nevládní organizací, či skupinou jednotlivců, které se považují za oběti v důsledku toho, že smluvní stát porušil ustanovení Evropské úmluvy či jejích protokolů.²⁶

Z hlediska ochrany soukromí a osobních údajů by bylo chybou přehlédnout článek 8 odst. 1 Evropské úmluvy, který říká: „*Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.*“ Druhý odstavec ve zkratce říká, že státní orgán obecně nemůže do výkonu tohoto práva zasahovat kromě vymezených důvodů, kdy je to v souladu se zákonem. Problémem druhého odstavce se zdá být to, že se v něm hovoří pouze o státních orgánech a nikoliv např. o zaměstnavatelích či jiných soukromých osobách. Pojem soukromý a rodinný život lze interpretovat i pomocí Rezoluce Rady Evropy 428 o masových komunikačních médiích a lidských právech z roku 1970, která chápe právo na soukromí jako právo, jež převážně spočívá v právu žít svůj vlastní soukromý a rodinný život s minimálními

²⁵ Tamtéž

²⁶ POTOČNÝ, MIROSLAV, ONDŘEJ, JAN *Mezinárodní právo veřejné – Zvláštní část*. 6. doplněné a rozšířené vydání. Praha: C.H. Beck, 2011, s. 114. ISBN 978-80-7400-398-1.

zásahy, bez odhalování jakýchkoliv nemístných či znevažujících skutečností a osobních informací, při zachování tělesné i mravní integrity.²⁷

Stejně jako v Deklaraci OSN je v článku 1 Dodatkového protokolu k Evropské úmluvě (1. dodatek) zakotvena garance každé fyzické i právnické osoby pokojně užívat svůj majetek, což je právo, které se v rámci pracovněprávního vztahu může dostat do rozporu s právem zaměstnance na soukromí. S ohledem na rozvoj technologií a neucelenou právní úpravu přijala Rada Evropy dvě rezoluce týkající se ochrany soukromí v elektronických souborech dat v soukromém²⁸ a ve veřejném sektoru.²⁹

Klíčovým dokumentem v oblasti zpracování osobních údajů v rámci Rady Evropy ovšem není výše uvedená Evropská úmluva, nýbrž Úmluva č. 108 o ochraně osob se zřetelem na automatické zpracování osobních dat ze dne 28. ledna 1981 („**Úmluva 108**“).³⁰ ³¹ Úmluva 108 se ve srovnání s tehdejšími dokumenty lišila především svojí závazností a také vysokou mírou konkrétnosti. Požadovaným cílem dle preambule tohoto dokumentu je dosažení větší jednoty mezi členskými státy, což v oblasti osobních údajů představovalo první výraznější krok k jejich mezinárodní ochraně, nepočítaje mezinárodní dokumenty týkající se ochrany lidských práv a základních svobod v obecní rovině.

²⁷ RADA EVROPY *Rezoluce 428. o masových komunikačních médiích a lidských právech* Dostupná z <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en> [cit. 13. 3. 2017]

²⁸ Council of Europe *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*. Dostupné z <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2> [cit. 13. 3. 2017]

²⁹ Council of Europe *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*. Dostupné z <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51> [cit. 13. 3. 2017]

³⁰ Sdělení Ministerstva zahraničních věcí o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. Sbírka mezinárodních smluv, částka 52 ročník 2001

³¹ pozn. Česká republika podepsala Úmluvu dne 8. září 2000 ve Štrasburku a po následném ratifikačním procesu vstoupila v platnost na území České republiky dne 1. listopadu 2001.

Účel Úmluvy 108 je stanoven v článku 1 a není jím nic jiného, než zaručit každé fyzické osobě na území smluvní strany „úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem na automatizované zpracování osobních údajů, které se k ní vztahují.“

Dle článku 3 se Úmluva 108 vztahuje na „*automatizované soubory osobních údajů a jejich automatizované zpracování ve veřejném a soukromém sektoru.*“ Za nedostatek Úmluvy 108 lze považovat právě její věcnou působnost, jelikož mnoho osobních údajů se zpracovává neautomatizovaně a z tohoto důvodu se tato Úmluva 108 nemůže aplikovat na veškeré zpracování osobních údajů.³² Nicméně smluvní státy mohou učinit prohlášení, že se Úmluva 108 uplatní i na soubory osobních údajů, které se nezpracovávají automatizovaně, tak ostatně učinila i Česká republika v roce 2005.³³

V ostatních člancích se Úmluva 108 věnuje, mj. definování několika základních pojmů, vymezení základních zásad pro ochranu osobních údajů či toku osobních údajů přes hranice.

K Úmluvě 108 byl vypracován Dodatkový protokol č. 1, jež vstoupil v platnost dne 1. července 2004. Cílem Dodatkového protokolu byla reakce na zvýšení toku informací mezi lidmi, jakož i zvýšené množství předávání osobních údajů přes hranice států. Na základě článku 1 Dodatku je každá smluvní strana povinna zřídit minimálně jeden nezávislý orgán dozoru odpovědný za dodržování příslušných opatření vnitrostátního práva s pravomocí vyšetřovat a zasahovat v důsledku porušení zásad týkajících se ochrany osobních údajů dle Úmluvy 108.

2.3 Evropská unie

Evropskou unii lze považovat za nadnárodní uskupení států, jež se odlišuje od standardních mezinárodních organizací či institucí vyšší mírou federalismu, která jde ruku v ruce s tím, že členské státy na ni přenesly výkon některých svých

³² MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 103. ISBN 978-80-7478-139-1.

³³ srov. Sdělení Ministerstva zahraničních věcí č. 29/2005 Sb. m. s.

pravomocí.³⁴ Z hlediska lidských práv a základních svobod je stěžejní Listina základních práv Evropské unie, která tvoří součást primárního práva EU.

Stejně jako Evropská úmluva, tak i Listina obsahuje v článku 7 právo na soukromý život a v článku 17 právo na vlastnictví majetku. Tvůrci Listiny základních práv EU, v komparaci s předchozími lidskoprávními dokumenty, vědomi si technologického rozvoje udělali poměrně výrazný krok v ochraně osobních údajů, kterou explicitně zakotvily v článku 8, jež stanoví: „Každý má právo na ochranu osobních údajů, které se ho týkají” (odst. 1); „Tyto údaje musí být zpracovávány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.” (odst. 2). Konečně v odstavci třetím je stanoveno, že na dodržování těchto pravidel dohlíží nezávislý orgán. Z citovaného ustanovení Listiny základních práv EU se nabízí srovnání s Úmluvou č. 108, a to zejména se zřízením nezávislého orgánu, který má provádět faktickou kontrolu a dohled nad dodržováním stanovených pravidel.

Smlouva o fungování Evropské unie upravuje v článku 16 (bývalý čl. 286 Smlouvy o ES) právo každého na ochranu osobních údajů, které se ho týkají a v druhém odstavci připravuje půdu pro Evropský parlament a Radu přijmout pravidla pro ochranu fyzických osob při zpracování osobních údajů. Tento článek v současnosti tvoří oporu nejen pro Směrnici Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů („**Směrnice**“), ale také pro Nařízení Evropského parlamentu a Rady 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**“).

Nejvýznamnější dokument v oblasti ochrany osobních údajů v rámci právní úpravy Evropské unie je stále výše uvedená Směrnice, která je tvořena 34 články,

³⁴ TOMÁŠEK, MICHAL, TÝČ, VLADIMÍR a kol. *Právo Evropské unie*. 1. Vydání. Praha: Leges, 2013, s. 55. ISBN 978-80-87576-53-3.

jímž předchází 72 recitálů, které vysvětlují sledovaný účel, cíl dané Směrnice a obecné zásady, čímž poskytují interpretační vodítko pro výklad následujících článků Směrnice.³⁵ Účel a cíl Směrnice tkví v harmonizaci právních předpisů, v ustavení rovnováhy mezi vysokou úrovní ochrany soukromí jednotlivců, volným pohybem osobních údajů v rámci Evropské unie či v zavedení nezávislého dozorového orgánu v každém členském státě.

Vzhledem k tomu že Směrnice byla do českého právního řádu implementována zákonem č. 101/2000 Sb., o ochraně osobních údajů, tak z metodologického hlediska budou působnost, základní pojmy či povinnosti subjektů předmětem následujících kapitol, které budou za opěrný bod považovat především tento zákon a dále budou také zmíněny některé významné změny provedené Obecným nařízením.

Směrnice ve svém článku 29 zřizuje nezávislou pracovní skupinu pro ochranu fyzických osob v souvislosti se zpracováním údajů („**WP 29**“) a upravuje organizační otázky této skupiny. Mezi hlavní úkoly WP 29 patří zejména posuzování veškerých otázek v souvislosti s národními předpisy provádějícími Směrnici za účelem jejich jednotného uplatňování či zaujímání stanoviska pro Komisi ohledně úrovně ochrany ve třetích zemích.

Od přijetí Směrnice uplynula poměrně dlouhá doba, která v oblasti informačních a jiných technologií plyne snad ještě rychleji než v reálném světě, a tak EU již od roku 2009 započala snahu o vytvoření nového, komplexnějšího rámce ochrany osobních údajů, který by držel krok s čím dál víc propracovanou výpočetní technikou a jejím prakticky celosvětovým rozšířením. Nepochybně dalším faktem byl rozvoj internetu a masové rozšíření sdílení osobních údajů skrz různé sociální sítě. Pro úplnost je dobré zmínit, že Směrnice sice vznikla v době, kdy internet ještě procházel svým vývojem a užívání moderních technologií bylo spíše ojedinělé, ale její obecnost dávala prostor pro interpretaci a přizpůsobení Směrnice na nové technologie.

³⁵ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 121. ISBN 978-80-7478-139-1.

V rámci diskusí došlo k rozdělení odborné veřejnosti do tří hlavních proudů, přičemž první z nich byl pro zachování současného stavu s upřesněním pravidel pro předávání osobních údajů, druhá skupina byla pro modernizaci Směrnice a konečně třetí, zvítězivší, skupina byla pro vypracování Obecného nařízení.³⁶

Obecné nařízení po přijetí Evropským parlamentem a Radou bylo dne 4. května 2016 vyhlášeno v Úředním věstníku Evropské unie, společně s trestněprávní směrní³⁷ a směrnicí o používání údajů jmenné evidence cestujících,³⁸ nabylo platnosti dvacátým dnem po jeho zveřejnění. V účinnost vstoupí dne 25. května 2018. Obecné nařízení představuje dle některých³⁹ revoluci v oblasti ochrany osobních údajů, dle autora této práce se jedná spíše o evoluci, a to s ohledem na to, že v mnohém navazuje na Směrnici a spíše posiluje ochranu osobních údajů, než že by zaváděla výrazné koncepční změny v této oblasti. Revoluce ovšem může být částečně spatřována např. ve zvolené formě právního předpisu EU, tedy úprava nikoliv ve směrnici, ale v nařízení, dále v ohlašování případů porušení zabezpečení osobních údajů či v neposlední řadě v zavedení funkce pověřence pro ochranu osobních údajů.

Otázkou je, zda je vhodné vůbec upravovat tuto problematiku na nadnárodní úrovni. Taková úprava je bezpochyby namístě u velkých poskytovatelů telekomunikačních a datových služeb či korporací typu Google a Facebook, jelikož

³⁶ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 153-154. ISBN 978-80-7478-139-1.

³⁷ Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 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

³⁸ Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti

³⁹ srov. BAJÁKOVÁ, EVA *Newsletter: Revoluce v právu ochrany osobních údajů bude v roce 2018* Dostupné z http://www.randalegal.com/download/files/newsletter_newsletter_revolucevprvuochranynosobnchdajid55084.pdf [cit. 20. 3. 2017]

odlišné národní úpravy by ohrožovaly volný pohyb těchto služeb a byly by jen málokdy dostatečně účinné.⁴⁰ Autor se plně ztotožňuje s kritikou Obecného nařízení ze strany Zdeňka Kühna, který tvrdí, že „*veřejnoprávní a tím méně evropská (veřejnoprávní) regulace svou povahou lokálních aktivit typu monitorovacích kamer na soukromých domech, sloužících k ochraně majetku provozovatelů těchto kamerových systému, smysl nedává.*“⁴¹ Veřejnoprávní regulace je v takových „malicherných“ případech velmi omezená, protože takových zpracovatelů dat je nesčetně mnoho a z toho důvodu je kontrola pouze selektivní a obvykle probíhá na základě různých udání.⁴²

Ve srovnání se Směrnicí je Obecné nařízení značně rozsáhlejší, obsahuje dokonce 173 recitálů a symbolických 99 článků. Dle druhého recitálu je „*cílem tohoto nařízení přispět k dotvoření prostoru svobody, bezpečnosti, práva a hospodářské unie, k hospodářskému a sociálnímu pokroku, k posílení a sblížení ekonomik v rámci vnitřního trhu a k dobrým životním podmínkám fyzických osob.*“ Zajímavou se zdá být i proklamace, že zpracování osobních údajů by mělo sloužit lidem. Recitály dále zmiňují např., v judikatuře již hojně užívanou, zásadu, že právo na ochranu osobních údajů není právem absolutním, a tak musí být v souladu se zásadou proporcionality v rovnováze s dalšími základními právy.

Obecné nařízení dle článku 1 „*stanoví pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů a pravidla týkající se volného pohybu osobních údajů.*“ Nadcházející odstavce napovídají, že cílem Obecného nařízení je chránit základní práva a svobody fyzických osob a jejich právo na ochranu osobních údajů. Stejně jako Směrnice, Obecné nařízení potvrzuje volnost pohybu osobních údajů v rámci EU.

Věcně se Obecné nařízení vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování údajů, obsažených

⁴⁰ KÜHN, ZDENĚK *Transformace pojmu soukromí na počátku třetího milénia*. Jurisprudence, 2017, č. 2, s. 3-11, ISSN 1802-3843

⁴¹ Tamtéž

⁴² Tamtéž

v evidenci a těch údajů, které do takové evidence mají být zařazeny. Vedle pozitivního vymezení působnosti je v následujícím odstavci vymezena i působnost negativní, tedy vymezení, kdy se Obecné nařízení neuplatní. Obecné nařízení se neuplatní například na zpracování prováděné fyzickou osobou v průběhu výlučně osobních či domácích činností, na zpracování za účelem prevence, odhalování či stíhání trestných činů.

Místně se Obecné nařízení vztahuje na zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii, a to bez ohledu na to, zda zpracování probíhá v Unii či mimo ni.⁴³

Z hlediska pracovněprávních vztahů je důležitý článek 88 Obecného nařízení, podle tohoto článku *„Členské státy mohou právním předpisem nebo kolektivními smlouvami stanovit konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, zejména za účelem náboru, plnění pracovní smlouvy včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, řízení, plánování a organizace práce, za účelem zajištění rovnosti a rozmanitosti na pracovišti, zdraví a bezpečnosti na pracovišti, ochrany majetku zaměstnavatele nebo majetku zákazníka, dále za účelem individuálního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru.“* Tato pravidla mají zahrnovat vhodná opatření zajišťující ochranu lidské důstojnosti, oprávněných zájmů a základních práv zaměstnanců (subjektů údajů).

Nutno dodat, že WP 29 stejně jako Směrnice bude nahrazena Obecným nařízením, které zavádí v článku 68 a násl. Evropský sbor pro ochranu osobních údajů („**Evropský sbor**“). Ten by měl přispívat k jednotnému uplatňování Obecného nařízení v celé Unii, např. poskytovat Komisi poradenství či podporovat spolupráci mezi dozorovými úřady.⁴⁴ Na rozdíl od WP 29, Evropský sbor bude mít právní subjektivitu a dozorové úřady budou v zásadě vázány jeho pokyny, doporučeními či

⁴³ Čl. 3 odst. 1 Obecného nařízení

⁴⁴ Recitál 139 Obecného nařízení

osvědčenými postupy.⁴⁵ Mimo to je Evropský sbor nadán určitou rozhodovací pravomocí, a to v případě sporů mezi dozorovými úřady.⁴⁶

Dalším počinem Evropské unie na poli osobních údajů je mimo jiné Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, která byla přijata v reakci na zvýšení frekvence výměny informací prostřednictvím veřejných služeb elektronických komunikací, jako je internet či telefonní služby.⁴⁷ Tato směrnice stanoví pravidla pro zajištění bezpečnosti dat, ohlašování narušení bezpečnosti či zákaz nevyžádaných sdělení bez souhlasu uživatele.

2.4 Česká republika

Jak již vyplývá z mezinárodní úpravy, tak ochrana osobních údajů spjatá s ochranou soukromí náleží mezi základní práva, a tak je jejich úprava obsažena i v ústavním pořádku České republiky.⁴⁸ Konkrétněji je pak úprava rozvedena v jednoduchém právu na zákonné úrovni. Hlavním právním předpisem v oblasti ochrany osobních údajů je bezpochyby zákon o ochraně osobních údajů,⁴⁹ dále se této problematiky dotýká také např. občanský zákoník⁵⁰ či trestní zákoník.⁵¹

Pro pracovněprávní vztahy představuje opěrný bod právní úpravy zákoník práce. I přesto ale nelze opomenout i některé zvláštní zákony, které se rovněž uplatní při zpracování osobních údajů v rámci pracovněprávních vztahů. Jedná se

⁴⁵ Čl. 68 a násl. Obecného nařízení

⁴⁶ Čl. 65 a násl. Obecného nařízení

⁴⁷ srov. Evropská Unie *Shrnutí legislativy EU*. Dostupné z <http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv%3A124120> [cit. 17. 3. 2017]

⁴⁸ srov. čl. 112 odst. 1 Ústavy: „*Ústavní pořádek České republiky tvoří tato Ústava, Listina základních práv a svobod, ústavní zákony přijaté podle této Ústavy a ústavní zákony Národního shromáždění Československé republiky, Federálního shromáždění Československé socialistické republiky a České národní rady upravující státní hranice České republiky a ústavní zákony České národní rady přijaté po 6. červnu 1992.*“

⁴⁹ Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

⁵⁰ Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

⁵¹ Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

mj. o zákon o zaměstnanosti,⁵² zákon o daních z příjmů,⁵³ zákon o důchodovém pojištění⁵⁴ či zákon o nemocenském pojištění.⁵⁵

2.4.1 Ústavní pořádek České republiky

Základní stavební kámen nejen svobody, ale i demokratického právního státu představuje článek 2 odst. 4 Ústavy, který obsahuje zásadu legální licence.⁵⁶ Tento ústavní princip spočívá ve svobodě každého činit vše, co není zákonem zakázáno.

V rámci ústavního pořádku je právo na soukromí a na ochranu osobních údajů upraveno v Listině základních práv a svobod („Listina“).⁵⁷ Článek 7 zaručuje nedotknutelnost osoby a jejího soukromí, přičemž omezena může být jen, stanoví-li tak zákon. Tento článek je rozveden následujícími články, které jsou k článku 7 v poměru speciality. Článek 10 upravuje právo každého, „*aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.*“ Druhý odstavec stanoví ochranu každého před neoprávněným zásahem do jeho soukromého a rodinného života. Konečně třetí odstavec upravuje právo na ochranu každého před neoprávněným užitím či zneužitím údajů o své osobě. Právě článek 10 lze z hlediska vnitrostátní právní úpravy považovat za základ ochrany soukromí.⁵⁸

Ochrana soukromí je částečně prolomena článkem 17, který stanoví svobodu projevu a právo na informace, a také povinnost státních orgánů a orgánů územní samosprávy přiměřeným způsobem poskytovat informace o své činnosti.

⁵² Zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů

⁵³ Zákon č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů

⁵⁴ Zákon č. 155/1995 Sb., o důchodovém pojištění, ve znění pozdějších předpisů

⁵⁵ Zákon. č. 187/2006 Sb., o nemocenském pojištění, ve znění pozdějších předpisů

⁵⁶ „*Každý občan může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá.*“

⁵⁷ Usnesení předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky

⁵⁸ WAGNEROVÁ, ELIŠKA in WAGNEROVÁ A KOL. *Listina základních práv a svobod – Komentář*. Praha: Wolters Kluwer, 2012, s. 280. ISBN 978-80-7357-750-6.

Z výše uvedeného vyplývá, že ochrana soukromí není neomezená a je-li ochrana zaručena vůči neoprávněným zásahům, tak zjevně musí existovat i zásahy oprávněné.⁵⁹

Ochrana osobních údajů a ochrana soukromí⁶⁰ se velmi často dostává do střetu s jiným ústavně zaručeným právem, jelikož formálně vzato není dle Listiny žádné lidské právo a základní svoboda nadřazeno jinému. V pracovněprávních vztazích nastává nejčastěji rozpor mezi ochranou osobních údajů zaměstnance a ochranou majetkových hodnot zaměstnavatele. Ústavní soud poskytl už v druhé polovině roku 1994 vodítko, jakým způsobem zvážit jakékoliv omezení základního práva či svobody. Tímto vodítkem je tzv. test přiměřenosti, který byl v té době znám jednak v doktríně,⁶¹ tak také v zahraniční judikatuře.⁶²

Test přiměřenosti se skládá z několika kritérií, které při střetu dvou ústavně zaručených práv a svobod pomohou vyřešit otázku, jaké právo má v daném případě přednost. Prvním je kritérium vhodnosti, tj. zda institut omezující určité právo, umožňuje dosáhnout sledovaný cíl (ochranu jiného základního práva).

Druhým je kritérium potřebnosti spočívající v porovnání prostředku omezujícího základní právo s jinými opatřeními, které umožňují dosažení stejného cíle bez zasažení do základních práv a svobod.

Třetím je kritérium závažnosti, pomocí jehož se porovnávají kolidující základní práva. Toto porovnání spočívá ve zvažování empirických, systémových, kontextových, ale také hodnotových argumentů.⁶³

⁵⁹ MAŠTALKA, JIŘÍ *Osobní údaje, právo a my*. 1 vyd. Praha: C. H. Beck, 2008, s. 6. ISBN 978-80-7400-033-1.

⁶⁰ pozn. ochrana osobních údajů a ochrana soukromí jako složky lidské důstojnosti

⁶¹ ALEXY, ROBERT A *Theory of Constitutional Rights*. Oxford: Oxford University Press, 2010, 516 s.

⁶² pozn. zejména judikatura Spolkového ústavního soudu v SRN

⁶³ Nález Ústavního soudu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94

2.4.2 Občanský zákoník

Občanský zákoník se v úvodních ustanoveních přihlašuje k zásadám, na jejichž základech je postaveno celé soukromé právo. Pro účely této práce je důležitá zejména zásada uvedená v § 3 odst. 2 písm. a), že „každý má právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí.“

Občanský zákoník dále v § 81 zakotvuje ochranu osobnosti člověka včetně všech jeho přirozených práv a povinnosti ctít svobodné rozhodnutí člověka žít podle svého. V druhém odstavci demonstrativně vyjmenovává hodnoty, které požívají ochrany, a to „život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy.“ Člověk, do jehož osobnosti bylo zasaženo, se může domáhat upuštění takového jednání či odstranění způsobeného následku.⁶⁴

Zachytit podobu člověka a rozšiřovat ji lze pouze s jeho souhlasem. Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.⁶⁵ Bez svolení člověka nelze, není-li dán zákonný důvod, narušovat jeho soukromé prostory, sledovat jeho soukromý život či pořizovat zvukové nebo obrazové záznamy o soukromém životě člověka.⁶⁶

Rozdíl mezi ochranou osobnosti a ochranou osobních údajů lze spatřovat v tom, že ochrana osobnosti představuje tradiční součást soukromého práva, kdežto úprava ochrany osobních údajů je veřejnoprávní regulací.⁶⁷ Ochrana osobnosti v občanském zákoníku může být chápána jako obecná úprava, která se aplikuje jak na oblast tělesné, tak také duševní integrity. Zatímco ochrana osobních údajů představuje zvláštní úpravu, která se aplikuje na kvalifikované nakládání s informacemi o fyzické osobě.⁶⁸

⁶⁴ § 82 odst. 1 občanského zákoníku

⁶⁵ §§ 84 - 85 občanského zákoníku

⁶⁶ § 86 občanského zákoníku

⁶⁷ NONNEMANN, FRANTIŠEK *Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů*. Právní rozhledy, C. H. Beck sv. 13-14/2012, s. 505. ISSN 1210-6410.

⁶⁸ Tamtéž

Co se pracovněprávních vztahů týče, tak se občanský zákoník užije, pakliže nelze použít zákoník práce. Subsidiarita soukromoprávního kodexu k zákoníku práce ovšem není bezbřehá a vždy musí být v souladu se základními zásadami pracovněprávních vztahů.⁶⁹

2.4.3 Zákon o ochraně osobních údajů

Ústředním zákonem v oblasti ochrany osobních údajů je, jak již samotný název napovídá, zákon ze dne 4. dubna 2000 č. 101/2000 Sb., o ochraně osobních údajů („**Zákon**“), který nabyl účinnosti dne 1. prosince 2000. Tento Zákon nahradil dle Jiřího Maštalky velmi zdařilý avšak praxí nerespektovaný zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.⁷⁰ Při tvorbě Zákona bylo nutné pamatovat na mezinárodněprávní závazky, které bylo nutné do Zákona zapracovat. Zejména se jedná o již zmiňovanou Úmluvu 108 a Směrnici, kterou Zákon ve velké míře následoval.

Předmětem samotného Zákona dle § 1 je upravit práva a povinnosti při zpracování osobních údajů a stanovit podmínky, za nichž je možné uskutečnit předání osobních údajů do jiných států. Mimo to Zákon také zřizuje ústřední správní úřad pro oblast ochrany osobních údajů, a to Úřad pro ochranu osobních údajů („**UOOU**“). Zákon dále definuje základní pojmosloví této problematiky, stanoví práva a povinnosti nejen správců či zpracovatelů, ale i subjektů zpracování. Autoritativnost Zákona je podpořena úpravou správního trestání, tedy přestupky fyzických osob a přestupky právnických osob a fyzických osob podnikajících.

Zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby, a to jak na automatické zpracování osobních údajů, tak i na zpracování jinými prostředky. Z hlediska pracovněprávních vztahů lze dojít k závěru, že se Zákon aplikuje i na každého zaměstnavatele a zaměstnance, pakliže zpracovávají osobní údaje. Zákon

⁶⁹ pozn. původně byl řešen vztah zákoníku práce a občanského zákoníku (z. č. 40/1964 Sb.) na principu delegace, tento princip byl nahrazen v návaznosti na Nález Ústavního soudu ze dne 12. 3. 2008, sp. zn. Pl. ÚS 83/06 principem subsidiarity

⁷⁰ MAŠTALKA, JIŘÍ *Osobní údaje, právo a my*. 1 vyd. Praha: C. H. Beck, 2008, s. 11. ISBN 978-80-7400-033-1.

se ovšem nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu a na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

Pro komparaci je dobré uvést i výše uvedenou úpravu věcné působnosti v Obecném nařízení, které „*se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.*“⁷¹

S ohledem na to, že k výkladu některých ustanovení Zákona dojde v následujících kapitolách této práce, tak v rámci této podkapitoly nebude Zákon detailněji rozebrán.

2.4.4 Zákoník práce

Jak již bylo uvedeno, ochranu soukromí a osobních údajů je nutné zajistit i v pracovněprávních vztazích, a to nejen z důvodu zásady zvláštní zákonné ochrany postavení zaměstnance. V pracovněprávních vztazích stojí na jedné straně zaměstnavatel jako správce osobních údajů a na druhé straně zaměstnanec jako subjekt údajů. Zaměstnavatel je na základě některých zákonů dokonce povinen zpracovávat osobní údaje, jindy se může rozhodnout využít možnosti zpracovávat, která je stanovena v právních předpisech, či se může rozhodnout pro zpracování, které není jakkoliv zákonem předepsané.

Z hlediska pracovněprávních vztahů lze zpracování osobních údajů rozdělit do několika fází dle toho, kdy ke zpracování dochází. První z nich tvoří zpracování osobních údajů před samotným vznikem pracovního poměru, následující fází je zpracování během trvání pracovního poměru a konečně poslední fází představuje zpracování osobních údajů po skončení pracovního poměru. Toto rozdělení bude předmětem jedné z následujících kapitol této práce.

Zpracování osobních údajů zaměstnavatelem je upraveno hned na několika místech zákoníku práce, např. se jedná o povinnost zaměstnavatele vést u jednotlivých zaměstnanců evidenci pracovní doby, povinnost evidovat pracovní

⁷¹ Čl. 2 Obecného nařízení

úrazy či vedení osobního spisu zaměstnance. Co se týče ochrany soukromí zaměstnance, tak opěrným bodem zákoníku práce je § 316, který upravuje jednak ochranu majetkových zájmů zaměstnavatele a opačně také ochranu osobních práv zaměstnance.

V prvním odstavci je upravena povinnost zaměstnance nepoužívat bez souhlasu zaměstnavatele jeho výrobní prostředky, a to včetně výpočetní techniky zaměstnavatele, který je oprávněn dodržování tohoto zákazu přiměřeně kontrolovat. Zaměstnavatel samozřejmě může na základě svého rozhodnutí stanovit podmínky, za nichž zaměstnanci mohou tyto pracovní prostředky užívat i pro osobní potřebu.

Tento odstavec neznamena nic jiného než vyjádření vlastnického práva zaměstnavatele podle článku 11 Listiny a § 1012 občanského zákoníku, které spočívá v možnosti libovolně nakládat se svým vlastnictvím a možnosti jiné osoby z toho vyloučit.⁷² Z tohoto důvodu je naprosto legitimní, aby zaměstnavatel mohl kontrolovat užívání svého majetku zaměstnanci. V opačném případě, kdy by taková kontrola byla zakázána a zaměstnanci by mohli užívat svěřené prostředky naprosto neomezeně, by došlo k porušení ústavně zaručeného vlastnického práva zaměstnavatele.

Druhý odstavec zakazuje zaměstnavateli narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele, a to buď podrobením zaměstnance „*otevřenému nebo skrytému sledování, odposlechu či záznamu telefonických hovorů zaměstnance, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.*“ Výjimku tvoří případ, kdy je dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. Následující odstavec upravuje povinnost zaměstnavatele přímo informovat zaměstnance o rozsahu takové kontroly a o způsobech jejího provádění.

Poslední odstavec § 316 obsahuje pravidlo, že zaměstnavatel nesmí vyžadovat od zaměstnance informace, jež nesouvisí s výkonem práce a se základním pracovněprávním vztahem.

⁷² MORÁVEK JAKUB *Sledování zaměstnanců v kontextu novely zákoníku práce*. Právní rozhledy, C. H. Beck sv. 5/2012, s. 175 a násl. ISSN 1210-6410

2.4.5 Trestní zákoník a ZTOPO

V neposlední řadě se této problematice věnuje i úprava trestního práva, která představuje prostředek *ultima ratio*, jenž se uplatní za předpokladu, že nepostačují prostředky jiných právních odvětví. V § 180 trestního zákoníku je zakotven trestný čin neoprávněného nakládání s osobními údaji. Tento trestný čin obsahuje 2 základní skutkové podstaty. Objektivní stránku tvoří pachatel, který „*neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.*“

Stejným způsobem bude potrestán i pachatel, který poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, čímž, stejně jako v první základní skutkové podstatě, způsobí dotčené osobě vážnou újmu.⁷³

Další trestné činy zajímavé z hlediska ochrany soukromí a osobních údajů představuje porušení tajemství dopravovaných zpráv či porušení tajemství listin a jiných dokumentů uchovávaných v soukromí.⁷⁴

Pachatelem těchto trestných činů může být jak fyzická osoba, v takovém případě se na ni bude vztahovat právě trestní zákoník,⁷⁵ tak také právnická osoba. V takovém případě se na ni uplatní zvláštní úprava zákona o trestní odpovědnosti

⁷³ srov. NONNEMANN, FRANTIŠEK *Trestní odpovědnost právnické osoby za neoprávněné nakládání s osobními údaji*. Právní rozhledy, C. H. Beck sv. 20/2016, s. 697 a násl. ISSN 1210-6410.

⁷⁴ §§ 182 – 183 trestního zákoníku

⁷⁵ pozn. na osobu, která v době spáchání činu překročila patnáctý rok a nepřekročila osmnáctý rok svého věku, se vztahuje zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů, ve znění pozdějších předpisů

právnických osob,⁷⁶ který v § 7 obsahuje výčet trestných činů, které právnické osoby⁷⁷ nemohou spáchat a výše uvedené trestné činy v tomto výčtu chybí.

⁷⁶ Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů („ZTOPO“)

⁷⁷ § 8 ZTOPO je stanovena přičitatelnost jednání jednotlivých osob, jednajících jménem, v zájmu nebo v rámci činnosti právnické osoby

3. Základní pojmosloví ochrany osobních údajů

Předmětem této kapitoly je vymezení některých základních pojmů v oblasti ochrany osobních údajů, jejichž pochopení je pro porozumění celé problematice ochrany osobních údajů naprostou nutností. Definice těchto pojmů mnohdy vychází z mezinárodních závazků, a to jak z Úmluvy 108, tak také ze Směrnice. Vzhledem k tomu, že v České republice se na tuto problematiku aplikuje Zákon, tak níže uvedené definice budou vycházet právě z tohoto právního předpisu s přihlédnutím k některým změnám, které přináší již platné Obecné nařízení.

V této kapitole nebudou vymezeny všechny pojmy, které Zákon obsahuje, ale jen ty, které autor považuje za nezbytné pro pochopení problematiky nebo ty, jejichž výklad přinesl v aplikační praxi problémy.

3.1 Osobní údaj

Osobní údaj představuje základní pojem celé problematiky ochrany osobních údajů, který je definován jako *„jakákoliv informace týkající se určeného nebo určitého subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“*⁷⁸

Pokud taková informace nespĺňuje výše uvedenou definici, tak není možné Zákon použít a dotčená osoba musí využít jiných právních prostředků.⁷⁹ Při určování identifikovatelnosti fyzické osoby je nutné přihlédnout ke všem prostředkům, které může správce nebo jiná osoba rozumně k takové identifikaci použít. K tomu je nutné vzít v úvahu objektivní faktory, jako jsou náklady a čas potřebný pro identifikaci s přihlédnutím k dostupným technologiím.⁸⁰

⁷⁸ § 4 písm. a) Zákona

⁷⁹ NONNEMANN, FRANTIŠEK in KUČEROVÁ, ALENA a kol. *Zákon o ochraně osobních údajů. Komentář*. 1 vydání. Praha : C. H. Beck, 2012, s. 50. ISBN 978-80-7179-226-0.

⁸⁰ srov. WP 29 *Opinion 4/2007 on the concept of personal data*. Dostupné z http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf [cit. 21. 3. 2017]

Shora uvedená definice navazující na Směrnici dokazuje, že tvůrci Směrnice vycházeli ze širokého pojetí tohoto pojmu. Důvodem se za prvé zdá být schopnost reagovat na technologické změny a za druhé schopnost postihnout pokud možno veškeré informace o určité či určitelné fyzické osobě.⁸¹

Tímto pojmem se zabývá stanovisko WP 29 č. 4/2007, které detailně rozebírá jednotlivé prvky definice. Jakákoliv informace dle uvedeného stanoviska WP 29 zahrnuje objektivní informace, jako je přítomnost určité látky v krvi, tak také subjektivní informace, tedy názory či hodnocení, např. „*Titius je dobrý pracovník a zaslouží si povýšení.*“⁸² Informace se považuje za osobní údaj bez ohledu na její pravdivost a pravidla ochrany osobních údajů zahrnují prostředky k nápravě nepravdivých informací.

Aby se jednalo o osobní údaj, tak se výše uvedená informace musí týkat určeného nebo určitelného subjektu údajů. Zatímco určenost je z hlediska gramatického výkladu považována za trvalou vazbu, tak určitelnost představuje proměnnou vazbu mezi informací a subjektem. Vztah mezi informací a konkrétním jednotlivcem vzniká pomocí určitých identifikátorů, které slouží k určení dané osoby.⁸³ Za přímou identifikaci se typicky považuje kombinace jména, příjmení a adresy. Subjekt může být ovšem identifikován i nepřímou, a to jakoukoliv jinou kombinací, která umožní od sebe odlišit jednotlivé fyzické osoby.

V druhé části definice je obsažen demonstrativní výčet druhů informací, které lze chápat jako osobní údaj. Nejedná se tedy pouze o identifikační údaje, např. jméno a příjmení, ale opravdu o všechny skutečnosti a informace o přímo či nepřímou určeném konkrétním jednotlivci. Do tohoto pojmu lze zahrnout i fyzické či fyziologické prvky jako je vzhled, výška, váha či barva vlasů, psychologické prvky jako jsou např. vlastnosti jednotlivce, ekonomické prvky např. výši příjmů dané osoby či sociální prvky identity jednotlivce.

⁸¹ pozn. dle rozsudku Soudního dvora EU ze dne 19. 10. 2016 ve věci C-582/14 Breyer proti Německo lze za osobní údaj považovat i IP adresu

⁸² srov. WP 29 *Opinion 4/2007 on the concept of personal data*. Dostupné z http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf [cit. 21. 3. 2017]

⁸³ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 200. ISBN 978-80-7478-139-1.

Z hlediska pracovního poměru, může být považováno za osobní údaj např. číslo zaměstnance, jelikož dle tohoto čísla je zaměstnavatel schopen bez vynaložení většího úsilí dohledat konkrétního jedince ve své databázi. Co se týče určení a určitelnosti subjektu údajů, tak bude vždy nutné u zaměstnavatele přihlídnout ke konkrétní povaze daného provozu. V případě zaměstnavatele, jehož pracoviště se nachází v menší kancelářské budově, bude termín údržbář zřejmě znamenat jednu konkrétní osobu a na základě tohoto druhu práce bude možné identifikovat daného jedince. Naopak ve velkém strojařském závodě bude údržbářů několik a k přesné identifikaci zaměstnance bude nutné přiřadit další identifikátor.

Nejvyšší správní soud v rozsudku čj. 9 As 34/2008 ze dne 12. února 2009 zmínil, že v dnešní vyspělé společnosti s rozvinutými elektronickými médii plná identita fyzické osoby znamená možnost tuto osobu určitým způsobem kontaktovat. Z tohoto důvodu *„se výklad pojmu „osobní údaj“ nemůže omezit striktně jen na znalost např. rodného čísla, adresy či pracoviště subjektu údajů. Z tohoto pohledu je za osobní údaj třeba považovat i číslo mobilního telefonu určité osoby, jakkoli může být takové číslo používáno příslušnou osobou jen dočasně.“* Tento rozsudek dokazuje, že soudy členských států jsou schopny svým výkladem reagovat na vyvíjející se technologie. Soud dále potvrdil široké pojetí osobního údaje a zdůraznil, že nelze pojem osobní údaj vázat jen na znalost „klasických“ osobních údajů např. rodného čísla či adresy bydliště subjektu.

Co se týče projevů osobní povahy ve smyslu § 81 odst. 2 občanského zákoníku, tak je nelze zaměňovat s pojmem osobní údaj ve smyslu Zákona. Tyto pojmy představují dva samostatné právní instituty, ačkoliv může docházet k jejich překryvu, např. podobizna jednotlivce bude předmětem obou pojmů.⁸⁴

Obecné nařízení definuje osobní údaje obdobně, a považuje za ně *„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,*

⁸⁴srov. UOOU Stanovisko č. 3/2012 – K pojmu osobní údaj. Dostupné z [https://www.uoou.cz/VismoOnline ActionScripts/File.ashx?id_org=200144&id_dokumenty=22546](https://www.uoou.cz/VismoOnline>ActionScripts/File.ashx?id_org=200144&id_dokumenty=22546) [cit. 21. 3. 2017]

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.“

Zajímavé jistě je to, že v demonstrativním výčtu informací, kdy je osoba identifikovatelná se nově nachází např. lokační údaje či síťový identifikátor. Z toho vyplývá, že autoři Obecného nařízení pamatovali při definování osobního údaje i na moderní technologie.

3.2 Citlivý osobní údaj

Kromě „běžných“ osobních údajů, zná Zákon po vzoru Směrnice, také zvláštní kategorii údajů, které označuje za údaje citlivé. Zpracování těchto údajů se ve srovnání se standardními osobními údaji považuje za více invazivní do soukromí jednotlivce a z tohoto důvodů pro ně Zákon stanoví přísnější režim.⁸⁵

Citlivé údaje jsou podmnožinou osobních údajů, a tak i v tomto případě musí takový údaj splňovat definici osobního údaje, tedy, že se taková informace vztahuje k identifikované či identifikovatelné fyzické osobě.⁸⁶ Při splnění této podmínky je dále nutné zkoumat, zda taková informace vypovídá o některé ze skutečností taxativně uvedených v § 4 písm. b) Zákona. Podle tohoto ustanovení se za citlivý údaj považuje „*osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů.*“ Dále se za citlivý údaj považuje biometrický údaj umožňující přímou identifikaci nebo autentizaci subjektu údajů. Ve zkratce lze říci, že se jedná o informace o původu člověka, jeho názorech a přesvědčení, dále informace o jeho osobním životě a genetické informace vztahující se k jeho osobě.

⁸⁵ srov. Důvodová zpráva k zákonu č. 101/2000 Sb., o ochraně osobních údajů [Systém ASPI]. Wolters Kluwer [cit. 19. 6. 2017]. ASPI_ID LIT14321CZ. Dostupné v Systému ASPI.

⁸⁶ NONNEMANN, FRANTIŠEK in KUČEROVÁ, ALENA a kol. *Zákon o ochraně osobních údajů. Komentář*. 1 vydání. Praha : C. H. Beck, 2012, s. 55. ISBN 978-80-7179-226-0.

Z hlediska pracovněprávních vztahů se může jevit problematickým zpracování hned několika z výše uvedených citlivých údajů. Mnohdy a to nejen mezi zaměstnavateli dochází k zaměnění pojmů národnosti a státního občanství, přičemž údaj o národnosti, tedy o příslušnosti fyzické osoby k určitému národu, je pro zaměstnavatele zpravidla irelevantní.⁸⁷ Naopak např. při zaměstnávání cizinců či v případě vyslání zaměstnance do České republiky je zaměstnavatel ze zákona povinen evidovat údaj o státním občanství daného zaměstnance.⁸⁸

Mezi citlivé údaje se řadí i informace o politických postojích fyzické osoby, lze tedy mezi citlivé údaje zahrnout i údaje o členství v politické straně či hnutí? Odpověď na tuto otázku se nezdá býti složitou, a to s přihlédnutím k tomu, že politické strany a hnutí se na veřejnosti prezentují určitým programem, kde se přinejmenším hlásí k nějakým hodnotám a ze samotného členství již vyplývá, že daná osoba alespoň část těchto hodnot a postojů se stranou či hnutím sdílí. Z tohoto důvodu by o „citlivosti“ takového údaje neměl být pochyb.

S odlišným názorem přišel Ústavní soud ve svém nálezu sp. zn. I. ÚS 517/10 ze dne 15. 11. 2010, v němž rozhodl, že: *„Údaj o členství jednotlivce v politické straně bez dalšího výše vymezené "kvality" tzv. citlivých údajů tedy nedosahuje. To platí v první řadě (tedy nejen) o údajích o členství soudce v KSČ ke dni 17. 11. 1989; jak bylo shora vyargumentováno, značí to výrazný přesah do sféry veřejné. Z povahy věci proto nemůže jít - v případě předmětného údaje - o informaci charakteru výlučně soukromého.“*

Citlivý údaj podle UOOU dále nepředstavuje také údaj o zdravotním stavu zaměstnance ve smyslu lékařského posudku vydaného poskytovatelem pracovnělékařských služeb, jelikož z takového posudku se zaměstnavatel dozví jen, jestli je daný zaměstnanec zdravotně způsobilý, nezpůsobilý, způsobilý s podmínkou, či zda pozbyl dlouhodobě zdravotní způsobilost.⁸⁹ Naopak, za citlivý údaj lze již

⁸⁷ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 208. ISBN 978-80-7478-139-1.

⁸⁸ srov. § 102 odst. 2 zákona. č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů

⁸⁹ ŠUBRT, BOŘVOJ, TUČEK, MILAN *Pracovnělékařské služby: Povinnosti zaměstnavatelů a lékařů*. 2. doplněné vydání Olomouc: ANAG, 2015, s. 160. ISBN 978-80-7263-944-1.

považovat informaci o tom, že zaměstnanec prodělal léčení ve specifickém zdravotním zařízení, např. v psychiatrické léčebně.⁹⁰

Obecné nařízení nově přináší definici údaje o zdravotním stavu, kterým jsou osobní údaje „*týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.*“⁹¹ Obecné nařízení také považuje údaj o zdravotním stavu za citlivý osobní údaj a obecně až na stanovené výjimky je zakázáno jejich zpracování. Jednu z výjimek, kdy je možné údaj o zdravotním stavu zpracovávat podle článku 9 odst. 2 písm. h) Obecného nařízení, představuje situace, kdy je „*zpracování nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance,...*“ Lze tedy dojít k podobnému závěru jako WP 29, že informace například o detailech nemoci, postižení, klinické léčbě nebo fyziologickém či biomedicínském stavu zaměstnance by měly být pro zaměstnavatele nedostupné a zakázané, naopak informace, že dotyčný zaměstnanec je dočasně práce neschopný či, že navštívil zubního lékaře na preventivní kontrole by se zaměstnavatel v zásadě dozvědět měl, a to i s ohledem na to, že taková nepřítomnost zaměstnance tvoří překážku v práci.⁹²

Jako problematické se v aplikační praxi ukázaly informace týkající se členství v odborových organizacích. Již výše uvedený § 316 zákoníku práce zakazuje zaměstnavateli požadovat od zaměstnance informace týkající se členství v odborové organizace. S tímto členstvím bývá obvykle spojeno placení odborářských příspěvků, které mnohdy zaměstnavatel přímo sráží odborově organizovaným zaměstnancům z jejich mzdy a následně je poukazuje na účet odborové organizace. V takovém případě ale zaměstnavatel zpracovává citlivý osobní údaj, a jelikož nelze takové zpracování podřadit pod jiný z právních titulů uvedených v § 9 písm. b) až i), tak podle písm. a) daného ustanovení, potřebuje výslovný informovaný souhlas

⁹⁰ srov. UOOU *Stanovisko č. 2/2012 – Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů*. Dostupné z https://www.uoou.cz/VismoOnline/ActionScripts/File.ashx?id_org=200144&id_dokumenty=3165 [cit. 25. 3. 2017]

⁹¹ Čl. 4 odst. 15 Obecného nařízení

⁹² srov. recitál 35 a 52 Obecného nařízení

zaměstnance a nutno dodat, že takové zpracování bude podléhat oznamovací povinnosti podle § 16 Zákona, jelikož není možné na takové zpracování uplatnit jakoukoliv z výjimek z oznamovací povinnosti dle § 18 Zákona.⁹³

Co se týče biometrických údajů, tak jejich schopnost bezchybně identifikovat osobu a zvýšená dostupnost přístrojů provádějících identifikaci vedla mnoho zaměstnavatelů k využívání zejména otisku prstů jako identifikátoru, jenž spolehlivě slouží k evidenci docházky zaměstnance či k otevírání vstupních dveří. Takové zpracování ovšem není bezproblémové a v pracovněprávních vztazích ho lze užít jen ve výjimečných situacích a přípustnost takového jednání bude také záviset např. na charakteru docházkového systému a možnosti přiřazení otisků prstů k jednotlivému zaměstnanci.⁹⁴

Zákon mezi citlivé údaje zařazuje také osobní údaj vypovídající o odsouzení za trestný čin.⁹⁵ Aby takový údaj šlo považovat za citlivý, musí být dotčená osoba za trestný čin opravdu odsouzena. Informace o podmíněném zastavení trestního stíhání či spáchání přestupku, tak nelze považovat za citlivý údaj. Zaměstnavatelé mohou za podmínek stanovených v zákoníku práce v návaznosti na speciální zákony po zaměstnancích vyžadovat výpis z rejstříku trestů jako důkaz o trestní bezúhonnosti zaměstnance.⁹⁶ Takový údaj není možné považovat za citlivý, jelikož bezúhonná osoba bude mít záznam v rejstříku trestů negativní. Pakliže by zaměstnanec předložil výpis z rejstříku trestů, který by obsahoval informace o odsouzení za trestný čin, tak by hypotéza citlivého údaje byla naplněna. Obecné nařízení již takový údaj formálně nezařazuje mezi údaje citlivé, ale i tak pro ně stanoví v článku 10 zvláštní režim zpracování.

⁹³ srov. UOOU *Stanovisko č. 2/2001 – Zpracování citlivého osobního údaje členských příspěvků v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací*. Dostupné z https://www.uoou.cz/files/stanovisko_2001_2-arch.pdf [cit. 25. 3. 2017]

⁹⁴ srov. WP 29 *Opinion 3/2012 on developments in biometric technologies*. Dostupné z http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [cit. 25. 3. 2017]

⁹⁵ NOVÁK, DANIEL *Zákon o ochraně osobních údajů a předpisy související. Komentář*. Praha: Wolters Kluwer, 2014, s. 102. ISBN 978-80-7478-665-5.

⁹⁶ NONNEMANN, FRANTIŠEK in KUČEROVÁ, ALENA a kol. *Zákon o ochraně osobních údajů. Komentář*. 1 vydání. Praha : C. H. Beck, 2012, s. 58-59. ISBN 978-80-7179-226-0.

Obecné nařízení upravuje zpracování zvláštních kategorií údajů v článku 9, který nově zařazuje mezi citlivé údaje také informaci o sexuální orientaci. Zákon i Směrnice sice považují údaj o sexuálním životě za citlivý osobní údaj, ale výslovné uvedení údaje o sexuální orientaci dosud v této kategorii údajů chybělo. Ve srovnání se Směrnicí Obecné nařízení mezi citlivé údaje zařazuje také genetické a biometrické údaje za účelem jedinečné identifikace fyzické osoby.⁹⁷ To ovšem nelze považovat za nějakou překotnou novinku, protože Zákon takové údaje mezi citlivé zařazuje již od tzv. euronovely.^{98 99}

3.3 Anonymní údaj

Zákon definuje anonymní údaj jako „*údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů.*“¹⁰⁰ Při určení, zda je osoba identifikovatelná, je podle třeba přihlídnout ke všem rozumně použitelným prostředkům, které mohou být použity ať už správcem či jakoukoliv jinou osobou, přičemž správce by měl vzít v úvahu dobu zpracování osobních údajů, jelikož je možné, že např. za 10 let bude technický vývoj umožňovat identifikování takové osoby na základě původně anonymního údaje¹⁰¹.

Otázkou ovšem zůstává, zda je v silách správce předpovídat technický vývoj a technologické možnosti v tak dlouhém časovém horizontu. Při striktním výkladu tohoto stanoviska WP 29 by správce musel veškeré údaje, které uchovává z opatrnosti považovat za osobní údaje, což nejen, že by bylo pro něj velmi obtížné,

⁹⁷ pozn. na rozdíl od Směrnice Zákon jak genetické, tak biometrické údaje zařazuje mezi citlivé údaje.

⁹⁸ Zákon č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

⁹⁹ srov. NONNEMANN, FRANTIŠEK a SKÁCELOVÁ, MICHAELA *Zpracování biometrických údajů ve světle obecného nařízení o ochraně osobních údajů (GDPR)* In: Epravo.cz [online]. Dostupné z: <https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-ve-svetle-obecneho-narizeni-o-ochrane-osobnich-udaju-gdpr-106028.html> [cit. 12. 7. 2017]

¹⁰⁰ Čl. 4 písm. c) Zákona

¹⁰¹ srov. WP 29 *Opinion 4/2007 on the concept of personal data*. Dostupné z http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [cit. 25. 3. 2017]

ale i proti smyslu Zákona, poněvadž lze zpracovávat osobní údaje jen v rozsahu nezbytném pro naplnění stanoveného účelu.

Anonymní údaj představuje pomyslný protipól osobního údaje a na takové údaje a jejich zpracování se Zákon nevztahuje. Proces, pomocí kterého se osobní údaj stane údajem anonymním, se nazývá anonymizace.

Obecné nařízení na rozdíl od Směrnice i Zákona výslovně zakotvuje pojem pseudonymního osobního údaje a proces, jenž se nazývá pseudonymizace. Pseudonymizace je takové zpracování osobních údajů, které již nemohou být přiřazeny k fyzické osobě bez použití dodatečných informací, které jsou uchovávány odděleně.¹⁰² Účelem pseudonymizace je omezení případných rizik, které souvisejí se zpracování osobních údajů. S pojmem anonymního údaje Obecné nařízení ve svých člancích nepočítá, jen v recitálu 26 zmiňuje, že se Obecné nařízení nevztahuje na anonymní informace.

3.4 Subjekt údajů

Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují. Tato definice může působit velmi jednoduše, ale přináší s sebou, jak je v právu obecně běžné, různé aplikační problémy. Jednu z otázek představuje, zda se za subjekt považuje i nasciturus či naopak osoba zemřelá.

První z uvedených modalit lze vyřešit poměrně snadno pomocí § 25 občanského zákoníku.¹⁰³ Vzhledem k tomu, že ochrana osobních údajů jednotlivce je nesporně v zájmu dítěte, tak je vhodné chránit jeho osobní údaje i před jeho narozením.¹⁰⁴

Druhá modalita ovšem představuje již složitější problém, kterému se věnuje i UOOU ve svém stanovisku č. 4/2012, kde říká: „*po úmrtí subjektu údajů pozbývají platnosti ta ustanovení zákona o ochraně osobních údajů, v nichž subjekt údajů*

¹⁰² Čl. 4 odst. 5 Obecného nařízení

¹⁰³ „*Na počaté dítě se hledí jako na již narozené, pokud to vyhovuje jeho zájmům. Má se za to, že se dítě narodilo živé. Nenarodí-li se však živé, hledí se na ně, jako by nikdy nebylo.*“

¹⁰⁴ srov. Důvodová zpráva k zákonu č. 101/2000 Sb., o ochraně osobních údajů [Systém ASPI]. Wolters Kluwer [cit. 19. 6. 2017]. ASPI_ID LIT14321CZ. Dostupné v Systému ASPI.

vystupuje jako účastník občanskoprávních vztahů, tedy ustanovení o právech subjektu údajů a povinnostech správce ve vztahu k subjektu údajů.“¹⁰⁵ Naopak ustanovení Zákona, kde subjekt údajů nevystupuje jako účastník občanskoprávních vztahů, zůstávají v platnosti.

Autor výše uvedené stanovisko nepovažuje za příliš šťastné, a to především z důvodu, že fyzickou osobou je pouze osoba, která je na živu, což lze ostatně dovodit i z § 23 občanského zákoníku podle kterého má člověk právní osobnost od narození až do smrti. Smrtí tak člověk ztrácí způsobilost mít v mezích právního řádu práva a povinnosti. Takové rozdělení nejen, že nemá oporu v právních předpisech, ale je také poměrně zmatečné a pro laika je prakticky nemožné taková ustanovení od sebe spolehlivě odlišit. V podobném duchu se k této problematice vyjádřila i WP 29, která ve svém stanovisku dále doplňuje, že i zemřelým osobám se v některých případech může dostat nepřímo určité ochrany.¹⁰⁶

Obecné nařízení v recitálu 27 stanoví, že se nevztahuje na osobní údaje zesnulých osob. V následující větě ovšem připouští, že členské státy mohou stanovit pravidla týkající se osobních údajů zesnulých osob. Autor se domnívá, že výše uvedená dvojkolejnost nemá jakékoli opodstatnění, a tak by se český zákonodárce neměl uchýlovat v této oblasti k jakékoli aktivitě.

S ohledem na shora uvedenou definici je zřejmé, že se za subjekt nepovažují osoby právnické, ovšem některé členské státy se rozhodly působnost některých ustanovení vztáhnout i na ně.¹⁰⁷ Český zákonodárce tyto státy nenásledoval a nerozšířil působnost na tyto osoby.

Otázkou však zůstává, zda lze považovat za subjekt dle zákona i fyzickou osobu podnikající. Ústavní soud se touto problematikou zabýval ve svém nálezu sp. zn. Pl. ÚS 38/02, kdy zmínil, že za rozlišovací kritérium je nutno považovat jejich

¹⁰⁵ srov. UOOU Stanovisko č. 4/2012 - *Zpracování osobních údajů zemřelých osob*. Dostupné z https://www.uoou.cz/files/stanovisko_2012_4_old.pdf [cit. 27. 3. 2017]

¹⁰⁶ srov. WP 29 *Opinion 4/2007 on the concept of personal data*. Dostupné z http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [cit. 25. 3. 2017]

¹⁰⁷ Tamtéž

podnikatelskou činnost a přirovnal tyto osoby k právnickým osobám. Takové rozhodnutí ovšem nelze podle názoru UOOU považovat za správné, protože dle stanoviska UOOU č. 3/2011, jednak právní argumentace Ústavního soudu není přesvědčivá a za druhé zejména v případě, „*kdy jednatel vykonává svobodné nebo obdobné povolání, je práce součástí jeho soukromého života.*“¹⁰⁸

Autor se spíše přiklání k názoru, který vyslovil Ústavní soud, že by rozlišovacím kritériem měla být skutečnost, zda daný subjekt vykonává podnikatelskou činnost a ne zvolená právní forma podnikání. Rozlišovací kritérium dle UOOU, tedy ve zkratce zda daná práce představuje součást soukromého života jednotlivce, je poměrně zavádějící, protože mnoho jednotlivců, kteří se účastní na chodu obchodní společnosti, ať už jako členové nejvyššího či statutárního orgánu, svojí prací doslova žijí a rovněž u nich tedy není možná spolehlivě rozlišit pracovní a soukromý život.

Podle názoru autora UOOU ve svém stanovisku nesprávně používá pojem tzv. osob samostatně výdělečně činných. Vhodnějším pojmem, který je všezahrnující a vystihuje lépe podstatu takové činnosti, je pojem podnikatel, kterým je ten: „*Kdo samostatně vykonává na vlastní účet a odpovědnost výdělečnou činnost živnostenským nebo obdobným způsobem se záměrem činit tak soustavně za účelem dosažení zisku, je považován se zřetelem k této činnosti za podnikatele.*“¹⁰⁹

Obecné nařízení již ve svém recitálu č. 14 explicitně stanoví, že se nevztahuje na zpracování osobních údajů právnických osob.¹¹⁰ V tomto případě Obecné nařízení nepřináší z hlediska české perspektivy žádné ujasnění a bude na výkladu, zda evropský zákonodárce myslel opravdu pouze právníké osoby, či podnikatele obecně.

¹⁰⁸ UOOU v této části odkazuje na rozsudek Nejvyššího správního soudu ze dne 5. listopadu 2009, sp. zn. 1 Afs 60/2009 – 119

¹⁰⁹ § 420 Občanského zákoníku

¹¹⁰ „*Ochrana poskytovaná tímto nařízením by se měla týkat zpracování osobních údajů fyzických osob bez ohledu na jejich státní příslušnost nebo bydliště. Toto nařízení se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právníké osoby, včetně názvu, právní formy a kontaktních údajů právníké osoby.*“

3.5 Zpracování osobních údajů

Zpracování osobních údajů je jedním z nejdůležitějších pojmů v této oblasti. Dle § 4 písm. e) Zákona je zpracováním osobních údajů „*jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky.*“ V druhé větě Zákon demonstrativně uvádí některé konkrétní, zřejmě nejčastější, operace, které lze zařadit pod pojem zpracování, jedná se o „*shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.*“

Pro připomenutí je dobré zmínit, že se Zákon nevztahuje na nahodilé shromažďování osobních údajů a z tohoto důvodu je nutné, aby ke zpracování docházelo systematicky, a to zejména u manuálního zpracování, jelikož u automatického zpracování je prvek systematickosti obsažen v samotné povaze takového zpracování.¹¹¹

Zákon řadí mezi další způsoby zpracování osobních údajů také shromažďování, uchovávání, blokování a konečně i likvidaci osobních údajů. Shromažďování představuje systematický postup, jehož úkolem je získání osobních údajů za účelem jejich uložení na nosič informací, a to pro jejich okamžité či pozdější zpracování. Zpravidla bude shromažďování představovat první krok, byť ne výlučně, při zpracování osobních údajů.¹¹² Nosičem zpracovávaných údajů může být jak papírový spis, např. osobní spis zaměstnance, tak také jeho případná elektronická verze uchovávána na pevném disku.

Další z úkonů, který může tvořit zpracování osobních údajů je jejich uchovávání. Legální definice vykládá uchovávání osobních údajů jako „*udržování údajů v takové podobě, která je umožňuje dále zpracovávat.*“¹¹³

¹¹¹ POSPÍŠIL, DANIEL in KUČEROVÁ, ALENA a kol. *Zákon o ochraně osobních údajů. Komentář.* 1 vydání. Praha: C. H. Beck, 2012, s. 68. ISBN 978-80-7179-226-0.

¹¹² Tamtéž, s. 71

¹¹³ § 4 písm. g) Zákona

Specifické případy zpracování osobních údajů tvoří jejich blokování a likvidace. Společným jmenovatelem těchto operací je to, že přicházejí v úvahu v situacích, kdy by dalším zpracováním osobních údajů docházelo či mohlo dojít k nezákonnému zásahu do osobnosti subjektu.¹¹⁴ K těmto úkonům může docházet, např. dojde-li k dosažení účelu zpracování nebo pokud správce zpracovává nepřesné údaje. K blokování osobních údajů či k jejich likvidaci může správce přistoupit na základě svého rozhodnutí, správního aktu či zákona.¹¹⁵

Blokování osobních údajů se od jejich likvidace odlišuje svojí dočasnou povahou, kdy správce na stanovenou dobu některé nebo všechny osobní údaje vyloučí z obvyklých operací zpracování.¹¹⁶

Konečné řešení při zpracování osobních údajů představuje právě jejich likvidace, která se považuje za nevratnou operaci, kdy dochází k fyzickému zničení jejich nosiče či k jejich fyzickému vymazání.¹¹⁷ Zlikvidované osobní údaje není možné jakýmkoliv způsobem obnovit.

Při likvidaci musí správce vzít v potaz veškeré možné následky, ke kterým může dojít. Nepostačí, pokud např. zaměstnavatel položí vedle přeplněné popelnice osobní spisy bývalých zaměstnanců. V takovém případě si tyto údaje může každý vzít, čímž by mohlo dojít k neoprávněnému zásahu do osobnosti subjektu údajů.¹¹⁸ Vhodným řešením se zdá být v takovém případě skartace takových spisů.

3.6 Správce

Další důležitý, ba dokonce možná jeden z nejdůležitějších, pojem představuje správce. Zákon považuje za správce „každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj.“

¹¹⁴ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 215-216. ISBN 978-80-7478-139-1.

¹¹⁵ Tamtéž, s. 74

¹¹⁶ NONNEMANN, FRANTIŠEK in KUČEROVÁ, ALENA a kol. *Zákon o ochraně osobních údajů. Komentář*. 1 vydání. Praha : C. H. Beck, 2012, s. 73. ISBN 978-80-7179-226-0.

¹¹⁷ § 4 písm. i) Zákona

¹¹⁸ srov. rozhodnutí UOOU ze dne 10. 3. 2004, č.j. 1233/03-3000/892/03-OLP

Správce tedy může být jak právnická osoba, stát, tak také osoba fyzická. Formálně vzato výše uvedená definice neodpovídá definici správce, která je uvedena ve Směrnici.¹¹⁹ Český zákonodárce nepřevzal kompletní definici ze Směrnice, a tak je při aplikaci nutné přihlídnout k eurokonformnímu výkladu.¹²⁰ V opačném případě by zákonná definice nepamatovala na správce, kteří zpracovávají osobní údaje ze zákona a z toho důvodu nemohou určit účel takového zpracování. Co se týče účelu zpracování osobních údajů, tak musí být vždy zákonný. Stanovení účelu lze rozdělit do 2 základních skupin.

Za prvé, účely zpracování jsou správci uloženy na základě zákona. Správce v takovém případě nemá, pakliže chce dodržet své zákonné povinnosti, na výběr, zda bude či naopak nebude osobní údaje zpracovávat. V pracovněprávních vztazích bude tento případ nejčastější, jelikož zaměstnavatel je dle mnoha zákonů správce osobních údajů *ex lege*. Zákonnost takového účelu lze sledovat již v samotném účelu zákonodárce takové zpracování provádět.¹²¹

Druhá skupina je tvořena správci, kteří ze své vlastní vůle určí účely zpracování osobních údajů. Z povahy věci je takové zpracování možné jen v horizontálních právních vztazích, jelikož v rámci těchto vztahů „každý může činit, co není zákonem zakázáno.“¹²² Nutno dodat, že i v tomto případě není možné zpracovávat osobní údaje naprosto libovolně a je nutné dodržet onu zákonnost, přičemž Zákon a v pracovněprávních vztazích také zákoník práce stanoví hranice pro takové zpracování. Nejčastěji dochází k takovému zpracování, a to nejen v pracovněprávních vztazích, za účelem ochrany majetku či oprávněných zájmů správce.

¹¹⁹ „správce“ [se rozumí] fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů; jsou-li účel a prostředky zpracování určeny právními a správními předpisy na úrovni jednotlivých států či Společenství, je možné určit správce nebo zvláštní kritéria pro jeho určení právem jednotlivých států nebo Společenství.“

¹²⁰ srov. rozsudek Soudního dvora ze dne 10. 4. 1984 ve věci 14/83, „Van Colson“

¹²¹ NONNEMANN, FRANTIŠEK in KUČEROVÁ, ALENA a kol. *Zákon o ochraně osobních údajů. Komentář*. 1 vydání. Praha : C. H. Beck, 2012, s. 78. ISBN 978-80-7179-226-0.

¹²² Čl. 2 odst. 3 Listiny

Určení prostředků zpracování znamená, že správce vymezení, jakými technickými způsoby bude k takovému zpracování docházet. Zákon rozlišuje automatizované zpracování, v tomto případě bude prostředkem zejména výpočetní technika a zpracování prováděné jinými prostředky, tedy např. vedení uspořádané kartotéky ve fyzické podobě.

Odpovědnost, je sice dle Zákona posledním definičním znakem, ovšem rozhodně ne znakem nepodstatným. Právě přidělení odpovědnosti správce za zpracování osobních údajů v plném rozsahu představuje pomyslnou nosnou zeď této definice a odlišuje správce od jiných subjektů.¹²³ Odpovědnost správce je jednak veřejnoprávní, tak také soukromoprávní.¹²⁴

Obecné nařízení ve svém článku 26 dále zakotvuje institut společných správců. Takoví správci se považují za společné správce, pakliže společně stanoví účely a prostředky zpracování. Společní správci si mezi sebou vymezí své podíly na odpovědnosti za plnění povinností podle Obecného nařízení.

3.7 Zpracovatel

Zpracování osobních údajů může správce vykonávat sám nebo může zmocnit nebo pověřit zpracovatele.¹²⁵ Zpracovatelem je tedy subjekt, který zpracovává osobní údaje na základě zvláštního zákona či pověření správce.

Zpracovatel je subjekt odlišný od správce, který se může na zpracování osobních údajů podílet. Z tohoto důvodu se za zpracovatele nepovažuje např. zaměstnanec, který provádí pro svého zaměstnavatele (správce) zpracování osobních údajů.

Existence zpracovatele je závislá, pomineme-li zákonné zmocnění,¹²⁶ na rozhodnutí přijatém správcem, který může na zpracovatele přenést část či veškeré

¹²³ srov. WP 29 *Opinion 1/2010 On the concepts of the „controller“ and „processor“*. Dostupné z http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf [cit. 1. 4. 2017]

¹²⁴ NONNEMANN, FRANTIŠEK in KUČEROVÁ, ALENA a kol. *Zákon o ochraně osobních údajů. Komentář*. 1 vydání. Praha : C. H. Beck, 2012, s. 80-81. ISBN 978-80-7179-226-0.

¹²⁵ § 4 písm. j) Zákona

své činnosti se zpracováním spojené. Stejně jako správcem, tak i zpracovatelem může být stát, právnická i fyzická osoba. Zpracovatel v takovém případě jedná pro správce, tj. slouží jeho zájmům.¹²⁷

Pakliže se správce rozhodne pověřit zpracováním osobních údajů zpracovatele, tak s ním o takovém zpracování osobních údajů musí uzavřít smlouvu v písemné formě, kde bude vymezen její rozsah, účel, doba a záruky, které přijme zpracovatel, týkající se zabezpečení ochrany osobních údajů.¹²⁸ Stejně jako správce, tak i zpracovatel je povinen dodržovat právní předpisy, zejména Zákon a rovněž nese za zákonnost zpracování vlastní odpovědnost.

Rozdíl mezi správcem a zpracovatelem činí zejména povinnost správce určit účel a prostředky zpracování osobních údajů a povinnost písemně oznámit zpracování Úřadu ještě před samotným zpracováním.

Obecné nařízení již od předcházející právní úpravy povoluje tzv. řetězení zpracovatelů, kdy zpracovatel přenáší část zpracování na další zpracovatele, a to v článku 28. Zpracovatel však může zapojit do zpracování dalšího zpracovatele jen se souhlasem správce. Dílčí zpracovatel musí, stejně jako „standardní“ zpracovatel poskytovat dostatečné záruky týkající se zavedení vhodných technických a organizačních opatření.

Autor považuje povolení řetězení zpracovatelů za správné a to s ohledem na to, že v dnešní době dochází k častému outsourcingu zpracovatelských operací na další subjekty. Zároveň úprava v Obecném nařízení i nadále dostatečně zachovává správci plnou kontrolu nad zpracováním tím, zda takové řetězení schválí či ne.

¹²⁶ např. § 3 a násl. zákona č. 133/2000 Sb., evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů

¹²⁷ srov. WP 29 *Opinion 1/2010 On the concepts of the „controller“ and „processor“*. Dostupné z http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf [cit. 1. 4. 2017]

¹²⁸ § 6 Zákona

3.8 Souhlas subjektu údajů

Správce může realizovat zpracování osobních údajů jen na základě právními předpisy uznaného důvodu – právního titulu.¹²⁹ Souhlas subjektu údajů představuje dle některých autorů preferovaný a základní právní titul pro zpracování osobních údajů.¹³⁰ S tímto tvrzením nelze plně souhlasit, jelikož Zákon v § 5 odst. 2 počítá i s případy, kdy lze zpracovávat osobní údaje i bez souhlasu subjektu.¹³¹ Tento nesprávný názor zřejmě vyplývá ze znění Zákona, které říká, že správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů a až poté jsou stanoveny „výjimky“, kdy lze zpracovávat osobní údaje i bez souhlasu subjektu údajů.¹³²

Nutno podotknout, že Směrnice,¹³³ ostatně jako Obecné nařízení,¹³⁴ považuje souhlas subjektu údajů za jeden z právních titulů zpracování osobních údajů a nikoliv

¹²⁹ MORÁVEK, JAKUB in HŮRKA, Petr a kol. *Zákoník práce a související ustanovení občanského zákoníku* 3. aktualizované a rozšířené vydání. Olomouc: ANAG, 2014, s.952

¹³⁰ srov. MAŠTALKA, JIŘÍ *Osobní údaje, právo a my*. 1 vyd. Praha: C. H. Beck, 2008, s. 48. ISBN 978-80-7400-033-1.

¹³¹ *Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,*

a) *jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce,*

b) *jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,*

c) *pokud je to nezbytné třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat,*

d) *jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem. Tím však není dotčeno právo na ochranu soukromého a osobního života subjektu údajů,*

e) *pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,*

f) *pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení, nebo,*

g) *jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona.*

¹³² § 5 odst. 2 Zákona

¹³³ Čl. 7 Směrnice

¹³⁴ Čl. 6 Obecného nařízení

za právní titul preferovaný. Autor tedy dochází k závěru, že tato častá mýlka je způsobena chybou českého zákonodávce, který do Zákona promítl nevhodným způsobem znění Směrnice. Možná i z tohoto důvodu se mnoho zaměstnavatelů snaží ospravedlnit jakékoli zpracování osobních údajů zaměstnanců jejich souhlasem i v případě, že je dán jiný právní titul. Takový postup vypovídá o nepochopení této problematiky a zaměstnavatelé by si měli uvědomit, že zaměstnanec může svůj souhlas kdykoliv odvolat. Dále má tento postup za následek také nesprávné informování zaměstnance (subjektu údajů) o zpracování jeho osobních údajů a v návaznosti na to nedostatečné plnění informační povinnosti správce, což podle § 45 odst. 1 písm. f) Zákona představuje přestupek, za který je možné obecně uložit sankci až do výše 5 milionů Kč.¹³⁵

Nutno podotknout, že v pracovněprávních vztazích dochází častěji ke zpracování osobních údajů bez souhlasu subjektu údajů než s jeho souhlasem. Souhlas až na pár výjimek nepřichází v úvahu v případě zpracování osobních údajů subjekty veřejného práva a v obligatorních věcech soukromého práva. Souhlas tedy přichází na řadu zejména v soukromoprávních fakultativních věcech, kdy se správce ze své vlastní vůle rozhodne provádět zpracování osobních údajů.

Souhlasem subjektu údajů se dle Zákona myslí svobodný a vědomý projev vůle, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.¹³⁶ Souhlas subjektu představuje právní jednání, kterým subjekt údajů uděluje správci oprávnění zpracovávat jeho osobní údaje. Z tohoto důvodu se, mimo náležitostí stanovených v Zákoně, uplatní také obecná ustanovení občanského zákoníku, který stanoví náležitosti takového projevu vůle.¹³⁷

Správce je dále povinen subjekt údajů při udělení souhlasu informovat o účelu zpracování, jaké údaje budou zpracovávány a po jakou dobu.¹³⁸ V praxi častá

¹³⁵ srov. UOOU Stanovisko č. 3/2014 – *K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícíu nesprávnému plnění informační povinnosti*. Dostupné z https://www.uouu.cz/assets/File.ashx?id_org=200144&id_dokumenty=22531 [cit. 10. 8. 2017]

¹³⁶ § 4 písm. n) Zákona

¹³⁷ § 545 a násl. občanského zákoníku

¹³⁸ § 5 odst. 4 Zákona

klauzule: „*souhlasím se zpracováním svých osobních údajů dle zákona o ochraně osobních údajů*,“ v žádném případě nesplní Zákonem stanovené náležitosti informovaného souhlasu.¹³⁹

Zákon, narozdíl od Směrnice, neklade požadavek výslovnosti takového souhlasu.¹⁴⁰ Konkludentní souhlas je tedy dle Zákona postačující formou. Neprojevením nesouhlasu ovšem nelze presumovat souhlas subjektu se zpracováním, jelikož Zákon požaduje svolení subjektu.¹⁴¹ I přes to lze správci doporučit zvolení vhodné formy souhlasu, zejména písemnou formu, jelikož po celou dobu zpracování musí být schopen prokázat tento souhlas.¹⁴²

K souhlasu subjektu údajů v pracovněprávních vztazích se také vyjádřila WP 29 ve svém stanovisku č. 8/2001, kde uvádí, že zpracování v pracovněprávních vztazích na základě souhlasu zaměstnance (subjektu údajů) by se mělo omezit jen na situace, kdy má zaměstnanec svobodnou volbu neudělit souhlas či svůj souhlas odvolat. Pokud by existovalo riziko újmy, typicky ztráta zaměstnání, tak zaměstnancem udělený souhlas nelze považovat za platný.

Dle názoru autora je problematika svobody projevu souhlasu se zpracováním osobních údajů zaměstnance poměrně složitá a nelze vytvořit jakousi „kuchařku“, kdy zaměstnanci hrozí nějaká újma a kdy ne. V těchto případech bude vždy záležet také na subjektivním vnímání zaměstnance a také na tom, jakým způsobem zaměstnavatel danou *ofertu* k udělení souhlasu podá zaměstnancům. Z toho by se dalo dojít k závěru, že zaměstnavatel by měl v ideálním případě zpracovávat osobní údaje svých zaměstnanců jen na základě právními předpisy stanovených titulů. Tuto dedukci ovšem nelze považovat za správnou, účelem Zákona totiž není omezit či vyloučit zpracování osobních údajů, nýbrž zavést pravidla pro jejich zpracování.

¹³⁹ srov. UOOU Stanovisko č. 2/2008 – *Souhlas se zpracováním osobních údajů*. Dostupné z https://www.uoou.cz/files/stanovisko_2008_2.pdf [cit. 1. 4. 2017]

¹⁴⁰ pozn. Zákon tento požadavek vyžaduje jen při souhlasu se zpracováním citlivých údajů dle § 9 písm. a)

¹⁴¹ Rozsudek Městského soudu v Praze ze dne 16. 10. 2012, sp. zn. 6 Ca 378/2008-37

¹⁴² § 5 odst. 4 Zákona

Obecné nařízení upravuje podmínky vyjádření souhlasu subjektu údajů podrobněji než Směrnice a Zákon. V článku 7 stanoví mimo výše uvedeného i nutnost odlišit udělení souhlasu od jiných skutečností uvedených na téže listině.¹⁴³ Typicky se může jednat o *ofertu* určité smlouvy, ve které bude muset být odlišitelně upraven samotný obsah smlouvy od ustanovení týkající se souhlasu subjektu. Obecné nařízení zvýšeně dbá na požadavek srozumitelnosti, přehlednosti a jednoduchosti právního jednání vůči subjektu údajů.¹⁴⁴

Obecné nařízení dále výslovně umožňuje subjektům údajů odvolat svůj souhlas, a to způsobem, který nesmí být obtížnější než samotné udělení souhlasu.¹⁴⁵ Předtím než subjekt údajů samotný souhlas udělí, musí být informován o možnosti takový souhlas odvolat.¹⁴⁶

¹⁴³ Čl. 7 odst. 2 Obecného nařízení

¹⁴⁴ Tamtéž

¹⁴⁵ Čl. 7 odst. 3 Obecného nařízení

¹⁴⁶ Tamtéž

4. Povinnosti zaměstnavatele a práva zaměstnance

V pracovněprávních vztazích z hlediska problematiky ochrany osobních údajů jsou role rozděleny poměrně jednoznačně. Na jedné straně vystupuje zaměstnavatel jako správce, jehož protiklad tvoří zaměstnanec, jako subjekt údajů. Zákon k naplnění svého účelu, tedy k ochraně soukromí,¹⁴⁷ stanoví správci mnohé povinnosti, které lze také chápat jako určitá práva subjektu údajů. Předmětem této části bude přiblížit některé základní povinnosti zaměstnavatele a s tím související práva zaměstnance.

4.1 Povinnosti správce osobních údajů a práva subjektu údajů

Úkolem zaměstnavatele jako správce jsou předně povinnosti, které musí splnit ještě předtím, než přistoupí k samotnému zpracování.¹⁴⁸ Jedná se zejména o povinnost stanovit účel, prostředky a způsob zpracování.

Jak bylo uvedeno již výše, tak obecně ne všichni správci musí určit účel zpracování. Správce nestanoví účel, pakliže mu povinnost zpracovávat osobní údaje vyplývá přímo ze zákona. Povinnost stanovit účel je jednou ze základních povinností podle Zákona, která předurčuje některé další povinnosti na účel navázané. Ať už správcem určený, nebo zákonem stanovený, účel musí být vždy zákonný a přesně vymezený.¹⁴⁹

Správce je povinen shromažďovat osobní údaje, které odpovídají stanovenému účelu, a to jen v rozsahu nezbytném a po nezbytně nutnou dobu k jeho naplnění.¹⁵⁰ Zpracovávané údaje musí být otevřené,¹⁵¹ přesné a aktualizované.

¹⁴⁷ § 1 Zákona

¹⁴⁸ pozn. podle § 7 Zákona povinnosti stanovené v § 5 Zákona platí obdobně také pro zpracovatele.

¹⁴⁹ NOVÁKOVÁ, LUDMILA in KUČEROVÁ, ALENA a kol. *Zákon o ochraně osobních údajů. Komentář*. 1 vydání. Praha : C. H. Beck, 2012, s. 101. ISBN 978-80-7179-226-0.

¹⁵⁰ K nezbytně nutné době k naplnění účelu při provozování kamerového systému srov. Stanovisko UOOU č. 1/2006 - *Provozování kamerového systému z hlediska zákona o ochraně osobních údajů*. Dostupné z https://www.uoou.cz/files/stanovisko_2006_1.pdf [cit. 24. 6. 2017]

¹⁵¹ pozn. je tedy vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti

Správce dále stanovuje prostředky a způsob zpracování osobních údajů, provádí samotné zpracování¹⁵² a samozřejmě za takové zpracování osobních údajů odpovídá.¹⁵³ Pokud správce provádí zpracování osobních údajů na základě zvláštního zákona, v pracovněprávních vztazích se typicky jedná o vedení mzdové a personální agendy, tak musí dbát na práva na ochranu soukromého a osobního života subjektu.¹⁵⁴

Další povinností správce jsou **povinnosti informační**. Správce musí při udělení souhlasu informovat subjekt o tom, „*pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období.*“¹⁵⁵

Subjekt údajů dále musí být při shromažďování osobních údajů informován o rozsahu a účelu zpracování, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny.¹⁵⁶ Aby mohl subjekt údajů efektivně využít svého práva na přístup k osobním údajům, práva na opravu osobních údajů či dalších práv stanovených v § 21,¹⁵⁷ tak musí být správcem o takové možnosti předem informován.

Pokud subjekt údajů požádá o informaci o zpracování svých osobních údajů, je mu správce povinen takovou informaci sdělit, a to bez zbytečného odkladu. Správce má právo za poskytnutí informace požadovat přiměřenou úhradu, která nesmí převyšovat nezbytné náklady na poskytnutí informace.¹⁵⁸

¹⁵² pozn. tím není dotčena možnost pověřit zpracováním zpracovatele

¹⁵³ K odpovědnosti správce více v bodě 3.6 této práce

¹⁵⁴ § 5 odst. 3 Zákona

¹⁵⁵ § 5 odst. 4 Zákona

¹⁵⁶ § 11 odst. 1 Zákona

¹⁵⁷ „Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může

a) požádat správce nebo zpracovatele o vysvětlení,

b) požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav, ...“

¹⁵⁸ § 12 Zákona

V případě, že subjekt údajů zjistí jakékoliv nesrovnalosti či jiný rozpor s ochranou soukromého a osobního života nebo rozpor se Zákonem, tak může požádat správce o vysvětlení či zjednání nápravy takového nežádoucího stavu.¹⁵⁹

Významné povinnosti správce se týkají také **zabezpečení** zpracovávaných osobních údajů. Správce je povinen „*přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.*“¹⁶⁰ S tím souvisí i povinnost zpracovat a dokumentovat provedená technicko-organizační opatření, která slouží k zajištění ochrany osobních údajů a povinnost posoudit potenciální rizika zpracování.¹⁶¹

Zákon sice v § 16 stanoví **oznamovací povinnost** pro správce, kteří hodlají zpracovávat osobní údaje, ale zároveň z této povinnosti stanoví výjimky. Oznamovací povinnost se nevztahuje zejména na zpracování osobních údajů na základě zvláštního zákona nebo na údaje potřebné k uplatnění práv a povinností vyplývajících ze zvláštního zákona.¹⁶²

Pokud tedy zaměstnavatel zpracovává osobní údaje svých zaměstnanců jen na základě zvláštních zákonů, např. za účelem již zmíněného vedení personální a mzdové agendy, tak v takovém případě nepodléhá oznamovací povinnosti vůči UOOU.¹⁶³ Obecně lze říci, že pokud bude zaměstnavatel vyžadovat od zaměstnanců ke zpracování souhlas, tak takové zpracování bude podléhat oznamovací povinnosti.

¹⁵⁹ § 21 Zákona

¹⁶⁰ § 13 odst. 1 Zákona

¹⁶¹ § 13 odst. 2 a 3 Zákona

¹⁶² § 18 Zákona

¹⁶³ srov. UOOU Stanovisko č. 6/2012 – Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů. Dostupné z https://www.uoou.cz/files/stanovisko_2012_6.pdf [cit. 20. 6. 2017]

Samotná oznamovací povinnost spočívá ve vyplnění elektronického formuláře,¹⁶⁴ kde se vyplní příslušné informace do příslušných kolonek¹⁶⁵ a následně se formulář odešle. V případě, že UOOU neshledá důvodnou obavu, že při oznámeném zpracování by mohlo dojít k porušení Zákona a oznámení obsahuje všechny náležitosti, tak UOOU uvedené informace zapíše do registru.

Stávající způsob plnění oznamovací povinnosti je zřejmě v rozporu s právními předpisy, jelikož takové oznámení nesplňuje veškeré náležitosti pro podání podle § 37 správního řádu.¹⁶⁶ Takové oznámení rovněž není žádným způsobem byt i elektronicky podepsáno a může ho učinit prakticky kdokoli, aniž by UOOU dokázal danou osobu verifikovat.

Pakliže správce řádně oznámil všechny náležitosti a UOOU nezahájil řízení, tak může po uplynutí 30denní lhůty zahájit zpracování. Zákon tak s nečinností správního orgánu spojuje fikci pozitivního „zapsání“ do registru a oznamovatel tak může zahájit samotné zpracování.¹⁶⁷ Samotná registrace tak má ze své povahy primárně evidenční funkci, tedy pouze zanést příslušné údaje do registru.

Nesplnění oznamovací povinnosti Zákon považuje za přešůpek, za který je možné uložit sankci až do výše 5 milionu Kč.¹⁶⁸ Pakliže by správce zpracovával osobní údaje naprosto v souladu se Zákonem a jen by opominul oznamovací povinnost, tak by společenská škodlivost takového protiprávního činu byla prakticky nulová a sankce by neměla být uložena. K nesplnění oznamovací povinnosti se vyjádřil také ústavní soud, který nepovažoval závažnost takového porušení za tak vysokou, aby měla za následek absolutní neúčinnost důkazu získaného průmyslovou kamerou.¹⁶⁹

¹⁶⁴ Elektronický formulář je dostupný na webových stránkách UOOU z <https://www.uou.cz/oznameni-o-zpracovani-osobnich-udaju.asp#obalhlava> [cit. 20. 6. 2017]

¹⁶⁵ § 16 odst. 2 Zákona

¹⁶⁶ Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů

¹⁶⁷ pozn. registrace není z hlediska správní vědy individuálním správním aktem

¹⁶⁸ podle § 45 odst. 1 písm. i) Zákona

¹⁶⁹ Usnesení Ústavního soudu ze dne 8. 2. 2010, sp. zn. IV. ÚS 2425/09

4.2 Obecné nařízení a změny v právech a povinnostech stran

Obecné nařízení, jak již bylo uvedeno, přináší zvýšenou ochranu osobních údajů. Co se práv subjektů týče, tak dle názoru autora, Zákon v komparaci s Obecným nařízením obstál a Obecné nařízení mnoho úplných novot nepřináší. Jednu z nich tvoří právo subjektu na přenositelnost svých údajů, tedy právo získat své osobní údaje od správce a možnost předat je dalšímu správci.¹⁷⁰

Obecné nařízení již výslovně zakotvuje právo na výmaz osobních údajů, které je známé z dosavadní judikatury také jako právo být zapomenut.¹⁷¹ Právo na výmaz prakticky znamená vyjádření povinnosti správce zlikvidovat za stanovených podmínek osobní údaje.¹⁷² Jedná se např. o situace, kdy osobní údaje již nejsou potřebné pro dané účely, subjekt údajů odvolá svůj souhlas nebo osobní údaje byly zpracovány protiprávně atd.¹⁷³

Velká pozornost je věnována také zabezpečení osobních údajů, kdy je nutné při posuzování vhodné úrovně bezpečnosti zohlednit veškerá rizika.¹⁷⁴ Zajímavou novinkou je ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu.¹⁷⁵ Tato povinnost spočívá v ohlášení jakéhokoliv porušení zabezpečení osobních údajů bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm správce dozvěděl, dozorovému úřadu.¹⁷⁶ Ohlášení není nutné, pakliže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

K zamyšlení jistě je i to, jak velkou vůli budou mít správci takové porušení zveřejňovat a vystavovat se riziku pokuty či „pošpinění“ svého jména, že nezacházeli, s osobními údaji subjektů vhodným způsobem. V takovém případě bude

¹⁷⁰ Čl. 20 Obecného nařízení

¹⁷¹ srov. rozsudek Soudního dvora EU ze dne 13. května 2014, ve věci C 131/12 Google Spain SL, Google Inc. Proti Agencia Española de Protección de Datos

¹⁷² Čl. 17 Obecného nařízení

¹⁷³ Tamtéž

¹⁷⁴ srov. čl. 32 Obecného nařízení

¹⁷⁵ srov. čl. 33 Obecného nařízení

¹⁷⁶ Tamtéž

záležet i na tom, jakou cestou se vydá dozorový úřad. Pokud dozorový úřad bude zvýšeně sankcionovat správce, kteří se snažili utajit své porušení a naopak „ulevovat“ správcům, kteří bezprostředně ohlásí jakékoliv porušení zabezpečení údajů, tak by tato povinnost mohla velmi efektivně fungovat a správci by mohli společně s pomocí dozorového úřadu zabránit dalším nežádoucím zásahům do práv subjektů údajů.

Taková úprava s sebou přináší několik otázek, např. kde se nachází hranice mezi tím, kdy je pravděpodobné riziko zásahu do práv a svobod jedince a kdy ne. Spolehlivě odpovědět na tuto otázku bude mnohdy velmi obtížným úkolem. Dle recitálu 75 mohou různě pravděpodobná a závažná rizika pro práva a svobody vyplynout ze zpracování osobních údajů, *„které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy by zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů chráněných služebních tajemstvím, neoprávněnému zrušení pseudonymizace nebo jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění, ...“* Další vodítko k určení pravděpodobnosti a závažnosti rizika pro práva subjektů lze najít v následujícím recitálu, dle něhož je nutné přihlídnout k povaze rozsahu, kontextu a účelům zpracování. Výše uvedený návod lze považovat za poměrně neurčitý a bude na výkladu, aby tento nepříliš jasný stav uspokojivě překlenul.

Otázkou také je, zda správce nebo i samotný pověřenec pro ochranu osobních údajů bude mít dostatečnou erudici k tomu, aby si takové porušení dokázal včas vyhodnotit a případně řádně podal ohlášení dozorovému úřadu.¹⁷⁷

Na to dále navazuje povinnost ohlásit takové porušení v případě, že zde bude vysoké riziko zásahu do práv a svobod fyzických osob a neuplatní se žádná z výjimek, také samotným subjektům údajů.¹⁷⁸

Nelze také opomenout, že Obecné nařízení již s dosavadní oznamovací povinností podle Zákona nepočítá. Ta je ale částečně nahrazena jinými povinnostmi,

¹⁷⁷ Čl. 33 odst. 3 Obecného nařízení

¹⁷⁸ Čl. 34 Obecného nařízení

kteře se obvykle týkají významného zpracování. Jednu z nich představuje povinnost správce a zpracovatele vést záznamy o činnostech zpracování.¹⁷⁹ V těchto záznamech má povinný subjekt uvádět Obecným nařízením stanovené informace, např. jméno a kontaktní údaje správce, účely zpracování či popis kategorie subjektu údajů. Tato povinnost se ovšem nevztahuje na podniky zaměstnávající méně než 250 osob, ledaže prováděné zpracování pravděpodobně představuje riziko pro práva a svobody subjektu údajů, zpracování není příležitostné, zahrnuje zpracování zvláštních kategorií údajů nebo údaje týkající se rozsudků v trestních věcech. Pokud dozorový úřad požádá o předložení záznamů o daném zpracování, tak je správce, zpracovatel či případný jejich zástupce povinen mu vyhovět a dané záznamy mu poskytnout.¹⁸⁰

Dle autora lze jistě pozitivně hodnotit výjimku pro „malé“ zaměstnavatele, pro které by taková povinnost mohla znamenat nadměrnou finanční i organizační zátěž. Otázku jistě také představuje stanovení hranice do 250 zaměstnanců, jelikož v evropském kontextu je určitě mnoho zemí, kde působí velké množství zaměstnavatelů s více než 250 zaměstnanci a naopak v některých zemích lze považovat zaměstnavatele např. s 200 zaměstnanci za opravdu velkého zaměstnavatele. Otázkou ovšem zůstává, jakým způsobem se při následné interpretaci a aplikaci Obecného nařízení vyloží nejen to, co znamená pravděpodobné riziko pro práva a svobody subjektu údajů, ale také význam příležitostného zpracování osobních údajů. Pokud bude následný výklad velmi striktní, tak se vlastně o žádné pozitivum nejedná a i menší zaměstnavatelé budou muset plnit tuto povinnost.

Další zajímavou otázkou představuje výklad toho, co znamená zpracování osobních údajů, které není příležitostné. Podle autora veškeré zpracování osobních údajů v rámci pracovněprávních vztahů je soustavné a striktně vzato by tak nebylo možné tuto výjimku uplatnit. S tím se ovšem nelze plně uspokojit, jelikož dle logického výkladu by pak daná výjimka nedávala moc smysl, protože by se prakticky nemohla uplatnit. Dle teleologického výkladu jistě nebylo účelem zákonodárce

¹⁷⁹ Čl. 30 Obecného nařízení

¹⁸⁰ Čl. 30 odst. 4 Obecného nařízení

vztáhnout tyto povinnosti i na velmi malé subjekty zaměstnávající jen pár zaměstnanců, a tak i podle tohoto výkladu je nutné se přiklonit spíše k názoru, že pokud hlavním předmětem činnosti zaměstnavatele není zpracování osobních údajů, tak lze takové zpracování považovat alespoň částečně za příležitostné. To ovšem nic nemění na tom, že tento výklad je poměrně kostrbatý a bude jistě zajímavé sledovat, jak se s tím aplikační praxe vypořádá.

Někteří správci budou v případě, že jejich zpracování, zejména při využití nových technologií, bude mít za následek vysoké riziko pro práva a svobody fyzických osob, povinni provést před zahájením zpracování posouzení vlivu na ochranu osobních údajů.¹⁸¹ Takové posouzení bude nutné provést především, pokud se jedná o (i) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatickém rozhodování, na němž se zakládají rozhodnutí; (ii) rozsáhlé zpracování zvláštní kategorie údajů či údajů týkajících se rozsudků v trestních věcech; (iii) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Takové posouzení musí obsahovat alespoň systematický popis zamýšlených operací zpracování a účely zpracování, posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů, posouzení rizik pro práva a svobody subjektu údajů či plánovaná opatření k řešení těchto rizik, a to včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s Obecným nařízením.¹⁸² Tato povinnost dle autora vyžaduje po správcích značné úsilí, aby nejen detekovali k jakému zpracování dohází, ale také, aby vyhodnotili a monitorovali jakékoliv aspekty daného zpracování. Tuto povinnost lze hodnotit pozitivně, a to z důvodu, že obecně vede k zajištění ochrany osobních údajů fyzických osob tím, že klade poměrně velké požadavky na daného správce. Ovšem je nutné zmínit, že za předpokladu, že by dozorové úřady sestavily a zveřejnily seznamy druhů operací zpracování, u nichž bude takové posouzení nutné ve velmi extenzivním rozsahu a i malé subjekty by byly povinny provádět takové zpracování, tak to pro ně může být velmi těžko únosné až možná likvidační.

¹⁸¹ Čl. 35 odst. 1 Obecného nařízení

¹⁸² Čl. 35 odst. 7 Obecného nařízení

Další povinnost, která se rovněž týká významného zpracování, představuje povinnost správce zkontrolovat s dozorovým úřadem dané zpracování, a to před jeho započítím. Tato povinnost nastává jen v případě, pokud po provedeném posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko, že by správce nepřijal opatření ke zmírnění tohoto rizika.¹⁸³

Novinkou je také povinnost v určitých případech jmenovat pověřence pro ochranu osobních údajů. Ten musí být jmenován vždy, kdy zpracování provádí orgán veřejné moci, přičemž zpracování tvoří hlavní činnost správce nebo zpracovatele a konečně při rozsáhlém pravidelném a systematickém monitorování subjektů údajů.¹⁸⁴ Tato povinnost se netýká každého správce, ale jen těch, kteří naplní výše uvedenou hypotézu. V případě, že ano, tak skupina podniků může jmenovat pouze jediného pověřence pro všechny své podniky.¹⁸⁵ Pověřenec může být jak zaměstnanec, tak také externí subjekt ve smluvním vztahu se správcem a měl by v oblasti ochrany údajů mít odborné znalosti a zkušenosti.¹⁸⁶

Úkolem pověřence je zejména poskytovat informace, poradenství správcům, monitorovat prováděné zpracování či komunikovat s dozorovým úřadem.¹⁸⁷ K řádnému výkonu pověřence jsou správce a zpracovatel povinni poskytnout pověřenci podporu a zapojit ho do veškerých záležitostí s ochranou osobních údajů souvisejících.¹⁸⁸

Obecné nařízení k tomu, aby byly dodržovány povinnosti, také upravuje složku represivní, spočívající v ukládání správních pokut. Hlavním rozdílem od předchozí úpravy v oblasti pokutování správců (zpracovatelů) je možná výše jednotlivých sankcí, která se může vyšplhat až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obrátu celosvětově za předchozí

¹⁸³ Čl. 36 Obecného nařízení

¹⁸⁴ Čl. 37 odst. 1 Obecného nařízení

¹⁸⁵ Čl. 37 odst. 2 Obecného nařízení

¹⁸⁶ Čl. 37 odst. 5 a 6 Obecného nařízení

¹⁸⁷ Čl. 39 odst. 1 Obecného nařízení

¹⁸⁸ Čl. 38 Obecného nařízení

finanční rok, podle toho, která hodnota je vyšší.¹⁸⁹ Takto vysoká výše možných pokut by mohla jako potenciální hrozba odstrašit správce a zpracovatele od ignorace této problematiky a motivovat je k zavedení postupů podle Obecného nařízení.¹⁹⁰

Mimo ukládání finančních sankcí upravuje Obecné nařízení v článku 58 odst. 2 písm. j) pravomoc dozorového úřadu udělit napomenutí správci či zpracovateli, jehož operace porušily Obecné nařízení. Recitál 148 toto ustanovení vykládá tak, že „v méně závažných případech porušení nebo pokud by pokuta, která bude pravděpodobně uložena, představovala pro fyzickou osobu nepřiměřenou zátěž, může být namísto pokuty uloženo napomenutí.“ Při ukládání sankcí je podle Obecného nařízení potřeba náležitě zohlednit jak povahu, závažnost a dobu trvání porušení, tak také případný úmysl, kroky učiněné ke zmírnění způsobené škody, míru odpovědnosti, případná předchozí porušení a způsob, jakým se dozorový úřad o daném porušení dozvěděl.¹⁹¹

Toto oprávnění nepředstavuje úplnou novinku, jelikož navazuje na čl. 28 odst. 3 Směrnice, který dozorovému orgánu dával pravomoc zaslat správci upozornění či napomenutí. Zákon ale takovou pravomoc neupravuje. Jako mírnější sankci ale Zákon upravuje v § 40 opatření k nápravě, které slouží k odstranění zjištěných nedostatků a stanoví lhůtu pro jejich odstranění. Pakliže dojde k nápravě protiprávního stavu podle uloženého opatření, tak může UOOU upustit od uložení pokuty.

Co se informační povinnosti týče, tak ji Obecné nařízení zpřesňuje a rozvádí. Zaměstnavatel je povinen své zaměstnance informovat o mnoha skutečnostech za použití jasných a jednoduchých jazykových prostředků, a to i za pomoci různých ikon. Dle názoru autora, je tento požadavek pro zaměstnavatele velmi obtížně řešitelný, protože na jedné straně stojí katalog povinností, které by měl zaměstnanec získat a naproti tomu požadavek jasnosti a transparentnosti. Pakliže by informace měla obsahovat Obecným nařízením požadované veškeré požadavky, tak se

¹⁸⁹ Čl. 83 odst. 5 Obecného nařízení

¹⁹⁰ pozn. jistě bude zajímavé sledovat, jakým způsobem stanoví český zákonodárce přepočty výše uvedených sankcí na CZK

¹⁹¹ Recitál 148 Obecného nařízení

rozhodně nevměštná, za použití standardně čitelné velikosti písma a fontu, na jednu stránku formátu A4. Podle názoru autora si Obecné nařízení vyloženě v této povinnosti protiřečí a bude zajímavé, jakým způsobem tyto povinnosti budou v následující aplikační praxi vykládány.

Drobnou úpravu přineslo Obecné nařízení i v právu subjektu na přístup ke svým osobním údajům. Subjekt údajů má podle článku 15 právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud ano, tak má právo získat k těmto osobním údajům přístup.¹⁹² Správce je dále povinen poskytnout subjektu kopie zpracovávaných osobních údajů.¹⁹³ Na rozdíl od Zákona, je správce povinen tyto informace poskytnout subjektu údajů zásadně bezplatně. Výjimku tvoří případy, kdy žádosti podané subjektem údajů jsou zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují. V takovém případě může správce buď (i) uložit přiměřený poplatek zohledňující administrativní náklad spojený s poskytnutím požadovaných informací nebo sdělení nebo učiněním požadovaných úkonů; nebo (ii) odmítnout žádosti vyhovět.¹⁹⁴

¹⁹² pozn. subjekt má právo získat přístup k těmto osobním údajům následujícím informacím jedná se o informace o:

- a) účely zpracování;
- b) kategorie dotčených osobních údajů;
- c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;
- d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
- e) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování a nebo vznést námitku proti tomuto zpracování;
- f) právo podat stížnost u dozorového úřadu;
- g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
- h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

¹⁹³ Čl. 15 odst. 3 Obecného nařízení

¹⁹⁴ Čl. 12 odst. 5 Obecného nařízení

5. Zpracování osobních údajů v jednotlivých fázích pracovního poměru

V této kapitole bude věnována pozornost jednotlivým zpracováním osobních údajů v pracovněprávních vztazích. Předmětem kapitoly nebude pouze zpracování osobních údajů za trvání pracovního poměru, ale i zpracování, ke kterému dochází před jeho vznikem či po jeho skončení. I přes to, že monitoring zaměstnanců lze systematicky zařadit do této kapitoly, tak vzhledem k jeho rozsahu je pro přehlednost vyčleněn do následující kapitoly.

5.1 Zpracování osobních údajů před vznikem pracovního poměru

Zpracování osobních údajů v rámci pracovněprávních vztahů nelze omezit pouze na dobu bezprostředního trvání pracovního poměru. Ke zpracování osobních údajů dochází již předtím, a to za účelem vybrání či získání vhodného budoucího zaměstnance z několika uchazečů.

Při výběrovém řízení zaměstnavatel obvykle zpracovává údaje uchazečů, které jim o sobě poskytli zasláním svých životopisů. Výběrové řízení probíhá obvykle tak, že zaměstnavatel na místě veřejně přístupném umístí svůj inzerát s nabízenými pozicemi, na který pak samotní uchazeči reagují zasláním svých životopisů. Právním titulem takového zpracování je § 5 odst. 2 písm. b) Zákona,¹⁹⁵ jelikož účelem takového zpracování je uzavření pracovní smlouvy. V praxi se lze setkat s názory, že po uzavření pracovní smlouvy s některým z uchazečů má zaměstnavatel zasláné životopisy neúspěšných uchazečů buď zlikvidovat, nebo uchazečům vrátit.¹⁹⁶

Z pohledu zaměstnavatele nelze tento přístup považovat za šťastný, jelikož neúspěšný uchazeč může výběrové řízení považovat za diskriminační a následně ho napadnout žalobou u soudu. Zaměstnavatel by bez dotčených životopisů jen velmi

¹⁹⁵ „jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů“

¹⁹⁶ JANEČKOVÁ, EVA, BARTÍK, VÁCLAV *Ochrana osobních údajů v pracovním právu (Otázky a odpovědi)*. Praha: Wolters Kluwer, 2016, s. 54. ISBN 978-80-7552-145-3.

těžko prokazoval, že vybral na danou pozici opravdu nejlepšího z kandidátů. Z tohoto důvodu lze zaměstnavatelům doporučit uchovávat zaslané životopisy jako případné důkazy i po skončení samotného výběrového řízení, a to po dobu příslušných promlčecích lhůt.¹⁹⁷

Rozsah informací, které může zaměstnavatel požadovat je velmi neurčitě vymezen v § 30 odst. 2 zákoníku práce, podle něhož zaměstnavatel smí vyžadovat jen informace, „*které bezprostředně souvisí s uzavřením pracovní smlouvy.*“ Do takové definice lze zahrnout i jiné informace než pouhé identifikační údaje potenciálního zaměstnance např. osvědčení o určitém vzdělání, rekvalifikačních kurzech či potvrzení o zaměstnání atd. V opačném případě by si zaměstnavatel mohl bez dalších informací jen velmi těžko vybrat nejlepšího z uchazečů.

Limitujícím faktorem samotného výběru je okruh informací, které zaměstnavatel nesmí od uchazečů požadovat, a to zejména podle § 316 odst. 4 zákoníku práce.^{198 199}

Podle tohoto ustanovení zaměstnavatel nesmí vyžadovat od zaměstnance informace, „*které bezprostředně nesouvisejí s výkonem práce.*“ Toto ustanovení pokračuje demonstrativním výčtem informací, které zaměstnavatel dokonce požadovat nesmí.

V daném výčtu je možné uvedené informace rozdělit do dvou skupin. První skupina obsahuje informace, které zaměstnavatel za žádných okolností nesmí vyžadovat. Ta je tvořena informacemi, které se týkají sexuální orientace, původu,

¹⁹⁷ pozn. v takovém případě je právním titulem § 5 odst. 2 písm. e) Zákona – ochrana práv a právem chráněných zájmů správce

¹⁹⁸ pozn. toto ustanovení lze považovat za generální ustanovení, které se uplatní i v prepracovní fázi

¹⁹⁹ pozn. č. 2 zákaz informací, které zaměstnavatel nesmí po zaměstnanci při výběru zaměstnanců požadovat je rovněž stanoven v § 12 odst. 2 zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů

členství v odborové organizaci, členství v politických stranách či příslušnosti k církvi nebo náboženské společnosti.²⁰⁰

Druhou skupinu tvoří informace, které může zaměstnavatel požadovat, pakliže je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána při zachování přiměřenosti takového požadavku. Do této skupiny zákoník práce zařazuje informace o těhotenství, rodinných poměrech, majetkových poměrech a trestněprávní bezúhonnost.

Zaměstnavatelé mnohdy požadují zejména od uchazeček informace, které se týkají jejich případného těhotenství či počtu a věku jejich dětí. Co se těchto informací týče, tak zaměstnavatelé je mohou požadovat, pakliže je pro to dán věcný důvod a pokud takové informace bezprostředně souvisejí s uzavřením pracovní smlouvy. Pokud daná pracovní pozice spočívá převážně ve vysílání zaměstnance na pracovní cesty, tak s ohledem na § 240 odst. 1 zákoníku práce,²⁰¹ nelze, dle názoru autora, po zaměstnavateli spravedlivě požadovat, aby upřednostnil těhotnou zaměstnankyni s rizikem, že mu i přes generální souhlas s vysíláním na pracovní cesty, odmítne v těhotenství a následně do 8 let věku dítěte takové vysílání. I přes to lze samozřejmě pochopit opačný přístup, který je více ochranářský vůči těhotným uchazečkám či obecně k podpoře rodiny.

Pakliže by se zaměstnavatel dotazoval na zakázané informace, tak zaměstnanec může bez jakéhokoliv postihu odpovědět nepravdivě.²⁰² Ve výše uvedeném případě, by uchazečka mohla nepravdivě odpovědět, že není těhotná, i když by ve skutečnosti byla, pokud by se jednalo o pracovní pozici, která není

²⁰⁰ Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů ve znění pozdějších předpisů stanoví v § 6 odst. 4 případy, kdy je legitimní požadovat informace týkající se příslušnosti k církvi nebo náboženské společnosti

²⁰¹ „Těhotné zaměstnankyně a zaměstnankyně a zaměstnanci pečující o děti do věku 8 let smějí být vysíláni na pracovní cestu mimo obvod obce svého pracoviště nebo bydliště jen se svým souhlasem; přeložit je může zaměstnavatel jen na jejich žádost.“

²⁰² srov. International Labour Organization *Code of practice on the protection of workers' personal data*. Dostupné z http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/--safework/documents/normativeinstrument/wcms_107797.pdf [cit. 27. 6. 2017]

těhotným zaměstnankyním zakázána či nespočívá ve vysílání na pracovní cesty (např. mzdová účetní).

Zajímavou otázku bezpochyby v prepracovní fázi z hlediska ochrany osobních údajů představují sociální sítě. Personalisté sami potvrzují, že při vyhledávání vhodných uchazečů stále častěji některé z nich používají.²⁰³ Vzhledem k tomu, že zaměstnavatel může požadovat od uchazečů jen omezené množství osobních údajů bezprostředně souvisejících s uzavřením pracovní smlouvy, tak jako neutrální lze považovat největší profesní sociální síť na světě LinkedIn, která slouží k setkávání osob diskutujících o profesních zájmech a k vyhledávání jednak nového zaměstnání, tak také nových zaměstnanců.

V této síti uživatelé obvykle veřejně na svých profilech sdělují profesní údaje o své osobě. Zejména se jedná o vzdělání, pracovní zkušenosti, napsané publikace či jazykové schopnosti, a to vše je samozřejmě doplněné poměrně uhlazenou fotografií uživatele. Z hlediska obsahu zveřejněných údajů se profil na této síti obvykle překrývá s životopisy uchazečů a zaměstnavatelé by tak neměli získat informace v rozporu se Zákonem.

Pomyslný protipól představuje na celém světě nejznámější sociální síť Facebook s více než dvěma miliardami registrovaných uživatelů, která slouží ke komunikaci mezi uživateli, udržování či navazování vztahů, sdílení dat a k mnoho dalším účelům.²⁰⁴ Na této síti již uživatelé sami sdílejí na své profilové zdi nejrůznější fotografie, videa, názory, příhody, komentáře či jinak vyjadřují své pocity. Mnoho uživatelů nedbá na ochranu svého soukromí a sdílí tyto údaje nejen mezi okruhem svých přátel, ale také veřejně pro kohokoliv.

Personalisté si mohou během několika sekund učinit o uchazeči naprosto jiný obrázek než ze zasláního životopisu či formálního pohovoru a následně vyřadit

²⁰³ srov. Česká televize *Fotka na Facebooku může uchazeči o práci podrazit nohy*. Dostupné z <http://www.ceskatelevize.cz/ct24/ekonomika/1564724-fotka-na-facebooku-muze-uchazeci-o-praci-podrazit-nohy> [cit. 24. 6. 2017]

²⁰⁴ Forbes *Mark Zuckerberg: 2 Billion Users Means Facebook's 'Responsibility Is Expanding'*. Dostupné z <https://www.forbes.com/sites/kathleenchaykowski/2017/06/27/facebook-officially-hits-2-billion-users/#551e09ab3708> [cit. 1. 7. 2017]

takového uchazeče vyřadit z výběrového řízení. Takový postup je ale v rozporu se Zákonem, otázkou však je, jakým způsobem lze zaměstnavateli vyřazení takového uchazeče na základě negativní zkušenosti s jeho profilem prokázat.

5.2 Zpracování osobních údajů v průběhu pracovního poměru

V průběhu trvání pracovního poměru dochází samozřejmě ke zpracování osobních údajů zaměstnanců v největším rozsahu. Údaje, které zaměstnavatel o svých zaměstnancích může shromažďovat, je možné rozdělit do tří kategorií.

První z nich tvoří obligatorní shromažďování osobních údajů, kdy zaměstnavatel nemá na vybranou a povinnost zpracovávat takové osobní údaje mu je uložena přímo právním předpisem, především v oblasti daňové či sociálního zabezpečení.²⁰⁵ Mnohé povinnosti také stanoví přímo zákoník práce. Typicky se jedná o povinnosti zaměstnavatele vést u jednotlivých zaměstnanců evidenci pracovní doby podle § 96 zákoníku práce.

Vedle údajů, které zaměstnavatel musí povinně shromažďovat, zde existuje i řada údajů, které zaměstnavatel nemá sice povinnost shromažďovat, ale uzná-li to za vhodné a účelné, tak takové zpracování může na základě právního předpisu provádět.²⁰⁶

Konečně třetí kategorii tvoří shromažďování osobních údajů zaměstnanců, které není v žádném právním předpisu předdefinováno. V takovém případě zaměstnavatel provádí zpracování osobních údajů svých zaměstnanců na základě vlastního rozhodnutí.²⁰⁷

Zákoník práce ve svém § 312 dává možnost zaměstnavateli vést **osobní spis** zaměstnance. Jelikož zaměstnavatel není povinen tento osobní spis vést, tak takové zpracování zařadíme právě do druhé výše uvedené kategorie.

²⁰⁵ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 386-387. ISBN 978-80-7478-139-1.

²⁰⁶ Tamtéž

²⁰⁷ Tamtéž

Obsahem osobního spisu mohou být jen písemnosti, které jsou „nezbytné pro výkon práce v základním pracovněprávním vztahu.“ Osobní spis typicky tvoří pracovní smlouva, potvrzení o zdravotní způsobilosti zaměstnance, osobní dotazník, mzdový výměr, různé informace pro zaměstnance, listiny prokazující účast zaměstnance na různých školeních či souhlas se zpracováním osobních údajů zaměstnance.

Do osobního spisu mohou nahlížet nejen vedoucí zaměstnanci, kteří jsou dotyčnému zaměstnanci nadřízeni, ale také některé státní orgány. Zákoník práce také pamatuje na zásadu přístupu subjektu údajů k informacím,²⁰⁸ a tak vedle výše uvedených osob může samozřejmě nahlédnout do svého osobního spisu i samotný zaměstnanec. Rozdíl mezi nahlédnutím do osobního spisu zaměstnancem a přístupem zaměstnance (subjektu údajů) ke svým osobním údajům podle Zákona, je v možnosti požadovat přiměřenou úhradu. Na rozdíl od běžného zpracování osobních údajů správcem, zaměstnavatel nesmí od svého zaměstnance požadovat jakoukoliv úhradu za nahlédnutí do svého osobního spisu.²⁰⁹

Údaj o mzdě či platu zaměstnance bývá i přes to, že formálně tato informace není zařazena mezi citlivé údaje dle § 4 písm. b) Zákona, velmi citlivě vnímána. Údaj o mzdě či platu ve spojení s konkrétním zaměstnancem je osobním údajem, a tak zaměstnavatelé jsou povinni o takovém údaji zachovávat mlčenlivost a zabezpečit ho proti jakémukoliv zveřejnění.²¹⁰ V České republice je, dle názoru autora, mzdová transparentnost teprve ve svém počátku, což může vést mimo jiné jen k velmi pomalému odbourávání rozdílů ve výši mezd mezi pohlavími. Naopak takové údaje jsou zakořeněny mezi lidmi jako údaje čistě soukromé a mnohdy je považováno až za neslušné tázat se druhých na výši jejich mzdy.

I přes výše uvedené, lze najít výjimky, kdy taková informace může být zpřístupněna i dalším osobám na základě právního předpisu. Jak bylo uvedeno výše,

²⁰⁸ srov. § 12 Zákona

²⁰⁹ § 312 odst. 3 zákoníku práce

²¹⁰ BARTÍK, VÁCLAV a JANEČKOVÁ, EVA *Poskytování osobních údajů o zaměstnancích*. Práce a mzda [online], 2010, č. 10. Dostupné z <http://www.mzdovapraxe.cz/archiv/dokument/doc-d26467v34836-poskytovani-osobnich-udaju-o-zamestnancich/> [cit. 27. 6. 2017]

tak některé státní orgány mohou nahlížet do osobního spisu zaměstnance, který bude zřejmě obsahovat i údaj o mzdě zaměstnance.²¹¹ Dále se může jednat o procesní předpisy, podle kterých je každý povinen sdělit soudu rozhodné skutečnosti pro dané řízení.²¹² Lze tedy uzavřít, že údaj o mzdě nelze zpřístupnit dalším osobám až na několik málo výjimek, kdy je tak stanoveno právním předpisem.

Zveřejňování platů je o poznání složitější problematikou, jelikož zde ochranu soukromí a osobních údajů částečně „prolamuje“ úprava zákona o svobodném přístupu k informacím („ZSPI“).²¹³ Původně státní orgány vykládaly ZSPI ve vztahu k údajům o platech zaměstnanců velmi restriktivně a většinu žádostí odmítaly.²¹⁴ Zlom nastal s rozhodnutím NSS sp. zn. 5 As 57/2010 – 79, podle kterého je zaměstnanec považován ve smyslu § 8b odst. 1 ZSPI za příjemce veřejných prostředků, protože dostává za svou práci plat z veřejných rozpočtů.^{215 216}

V návaznosti na tento rozsudek UOOU vydal společně s Ministerstvem vnitra „Metodické doporučení k poskytování informací o platech pracovníků povinných subjektů podle zákona o svobodném přístupu k informacím,“ které poskytuje vodítko při zveřejňování údajů o platu.²¹⁷ Tato metodika vykládá výše uvedený rozsudek tak, že po zohlednění všech okolností konkrétního případu, lze v určitých případech i nadále takovou žádost odmítnout. V každém jednotlivém případě, tak bude

²¹¹ Tamtéž

²¹² např. § 128 zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů či § 8 zákona č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů

²¹³ Zákon č. 106/1999 Sb.

²¹⁴ JANEČKOVÁ, EVA, BARTÍK, VÁCLAV *Ochrana osobních údajů v pracovním právu (Otázky a odpovědi)*. Praha: Wolters Kluwer, 2016, s. 74. ISBN 978-80-7552-145-3.

²¹⁵ Rozsudek Nejvyššího správního soudu ze dne 27. května 2011, sp. zn. 5 As 57/2010 - 79

²¹⁶ srov. NONNEMANN, FRANTIŠEK a FOLDOVÁ, VANDA *Zveřejňování platů zaměstnanců veřejné sféry ve světle aktuálního rozsudku Nejvyššího správního soudu*. Právní rozhledy, C. H. Beck sv. 2/2015, s. 63 a násl. ISSN 1210-6410.

²¹⁷ UOOU a MVČR *Metodické doporučení k poskytování informací o platech pracovníků povinných subjektů podle zákona o svobodném přístupu k informacím*. Dostupné z <https://www.uouu.cz/files/Metodika.pdf?p1=3308> [cit. 27. 6. 2017]

poskytnutí takové informace záviset zejména na úrovni pozice daného zaměstnance a na tom, jak moc velký je veřejný zájem na takové informaci.²¹⁸

Osobní údaje zaměstnanců na webových stránkách zaměstnavatele.

Posílení transparentnosti ve vztahu ke klientům či zákazníkům či vlastní sebeprezentace obvykle vede zaměstnavatele ke zveřejňování různých informací o zaměstnancích na svých webových stránkách. Na webových stránkách se obvykle objevuje jméno, příjmení, pracovní pozice e-mailová adresa, specializace či jazyková vybavenost zaměstnance.

Co se výše uvedených údajů týče, tak zaměstnavatel nepotřebuje souhlas zaměstnance, jelikož se zde uplatní § 5 odst. 2 písm. e) Zákona, tedy, že bez souhlasu subjektu lze osobní údaje zpracovávat, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby. Takové zpracování může být potřebné k plnění úkolů zaměstnavatele, ale i tak zaměstnavatel musí šetřit soukromí zaměstnance a nezveřejňovat např. jeho soukromé telefonní číslo či jeho bydliště.²¹⁹

Vedle výše uvedených údajů zaměstnavatelé mnohdy zveřejňují na svých webových stránkách i portrétní fotografie svých zaměstnanců. V takovém případě je obtížné najít nějakou z výjimek, kdy není potřeba souhlas zaměstnance a zřejmě není možné tvrdit, že takové zpracování je nezbytné pro ochranu práv a právem chráněných zájmů správce, jelikož k samotné reprezentaci zaměstnavatele či transparentnosti vůči klientům postačí (např. k rozhodnutí, zda se obrátí na zaměstnavatele s určitou zakázkou) výše uvedené informace, a proto bude nutné požádat zaměstnance o jeho souhlas.

Otázkou ovšem je, zda dané zpracování bude vůbec nezbytné pro naplnění daného účelu. Takové zpracování osobních údajů bude prováděno zřejmě za marketingovými účely. Dle § 5 odst. 1 písm. d) je správce povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro

²¹⁸ Tamtéž

²¹⁹ JANEČKOVÁ, EVA, BARTÍK, VÁCLAV *Ochrana osobních údajů v pracovním právu (Otázky a odpovědi)*. Praha: Wolters Kluwer, 2016, s. 68-71. ISBN 978-80-7552-145-3.

naplnění takového účelu. Je ovšem nezbytné z důvodu marketingových aktivit zveřejňovat fotografie zaměstnanců? Vybírají si klienti či zákazníci zaměstnavatele snad z důvodu vzhledu jeho zaměstnanců? Dle názoru autora takové zveřejnění fotografií zaměstnanců rozhodně není pro daný účel nezbytné a zákazníkům či klientům budou stačit případně údaje jako je osobní jméno a příjmení či kontaktní údaj např. e-mail či telefonní kontakt na daného zaměstnance.

Při striktním výkladu Zákona by se dalo dojít k závěru, že se souhlas subjektu údajů uplatní jen ve velmi výjimečných situacích, kdy nelze uplatnit žádný jiný právní titul zpracování a za předpokladu nezbytnosti takového zpracování. S tím ovšem nelze plně souhlasit, jelikož dle názoru autora, účelem zákonodárce nebylo prakticky zakázat užití souhlasu jako právního titulu, ale pouze omezit excesy, kdy se zpracovávají osobní údaje, které absolutně nesouvisí s daným účelem.

5.3 Zpracování osobních údajů po skončení pracovního poměru

Ačkoli zákoník práce označuje pracovněprávní vztahy za vztahy vznikající při výkonu závislé práce, tak by bylo chybou omezit povinnosti zaměstnavatele týkající se zpracování osobních údajů jen na dobu trvání pracovního poměru či dobu tomu bezprostředně předcházející. I přes to, že zaměstnavatel může zpracovávat osobní údaje pouze po dobu nezbytnou k naplnění účelu zpracování (z povahy věci se jedná o dobu trvání pracovního poměru), tak některé právní předpisy stanoví povinnost archivovat určité údaje pro případné prokázání řádného plnění povinnosti v oblasti sociálního zabezpečení či v daňové oblasti.²²⁰ V takovém případě je právním titulem zpracování § 5 odst. 2 písm. a) Zákona.²²¹ V některých případech je zaměstnavatel povinen archivovat určité dokumenty až po několik desítek let.²²²

Ve vlastním zájmu může zaměstnavatel archivovat údaje sloužící k případné jeho obraně v případě sporu o neplatnost rozvázání pracovního poměru či proti

²²⁰ srov. UOOU *Ke zpracování osobních údajů bývalých zaměstnanců*. Dostupné z <https://www.uoou.cz/ke-zpracovani-osobnich-udaju-byvalych-zamestnancu/d-1585> [cit. 27. 6. 2017]

²²¹ „zpracování nezbytné pro dodržení právní povinnosti správce“

²²² např. zaměstnavatel má povinnost uchovávat mzdové listy po dobu 30 kalendářních roků po příslušném roce podle § 35a odst. 4 písm. d) zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení

obvinění z diskriminačního jednání.²²³ Pokud by si zaměstnavatel takové údaje neuchoval, tak by v případě sporu byla jeho obrana značně oslabena. Doba takového uchování je navázána na příslušné promlčecí lhůty.

Při skončení pracovního poměru je zaměstnavatel povinen vydat zaměstnanci **potvrzení o zaměstnání**, ve kterém uvede zákoníkem práce stanovené údaje.²²⁴ Na rozdíl od pracovního posudku, potvrzení o zaměstnání se vydává obligatorně a neobsahuje žádné subjektivní hodnocení zaměstnance.

Pracovní posudek je zaměstnavatel povinen vydat do 15 dnů od žádosti zaměstnance. Obsahem takového posudku jsou již „*veškeré písemnosti týkající se hodnocené práce zaměstnance, jeho kvalifikace, schopností a dalších skutečností, které mají vztah k výkonu práce.*“²²⁵

Zákoník práce dává zaměstnanci možnost napadnout obsah potvrzení o zaměstnání nebo pracovního posudku u soudu v případě, že s ním nesouhlasí, a to do 3 měsíců ode dne, kdy se o takovém obsahu dozvěděl.²²⁶

6. Sledování zaměstnanců

Jak již bylo uvedeno v úvodních kapitolách této práce, tak soukromí je třeba chápat nejen v rovině osobní sféry jednotlivce, ale také v právu každého člověka na vytváření a rozvíjení vztahů s dalšími jedinci. Takové právo ale není právem neomezeným a mnohdy se dostává do střetu s legitimními zájmy zaměstnavatele, který se snaží chránit svůj majetek či kontrolovat zda zaměstnanci využívají pracovní dobu k výkonu práce. V jednotlivých případech je vždy nutné řádně uvážit, které právo převáží nad druhým.²²⁷

²²³ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 388. ISBN 978-80-7478-139-1.

²²⁴ § 313 zákoníku práce

²²⁵ § 314 zákoníku práce

²²⁶ § 315 zákoníku práce

²²⁷ ke sledování zaměstnanců srov. MORÁVEK JAKUB *Sledování zaměstnanců v kontextu novely zákoníku práce*. Právní rozhledy, C. H. Beck sv. 5/2012, s. 175 a násl. ISSN 1210-6410.

S vývojem informačních a komunikačních technologií přišly nejenom nové vymoženosti, které usnadňují a urychlují práci zaměstnanců, ale také značná rizika. Jedním z největších rizik práva zaměstnance na soukromí je možnost zaměstnavatele sledovat jeho elektronickou poštu, činnost na internetu, telefonní hovory a v neposlední řadě monitorovat jeho činnost kamerami.

Kontrolu zaměstnanců nelze považovat za negativní jev, protože dle autora nepochybně patří k jednomu z rysů závislé práce. Kdyby zaměstnavatel nemohl kontrolovat práci svých zaměstnanců, tak si lze snadno představit, jakým způsobem by práce zaměstnanců (ne)vypadala, a tak zákoník práce samozřejmě takovou kontrolu umožňuje.²²⁸ Z pohledu zaměstnance by sice taková nemožnost kontroly, mohla znít hezky, ale je třeba si uvědomit, že kontrola a hodnocení zaměstnance přináší zaměstnanci nezbytnou zpětnou vazbu, bez níž by se zaměstnanec jen velmi těžko posouval kupředu a jeho pracovní výkon by přinejlepším stagnoval. Otázkou tedy není, zda může zaměstnavatel své zaměstnance kontrolovat, ale co vše může kontrolovat, v jakém rozsahu a jakým způsobem.

Středobodem ochrany osobních práv zaměstnance je již zmiňovaný § 316 odst. 2 zákoníku práce, který sice zaměstnavateli dává možnost zavést kontrolní mechanismy, ale jen za předpokladu, že je dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. Taková kontrola tedy nemusí být jen výlučně ku prospěchu zaměstnavatele (např. k ochraně jeho majetku), ale také např. k ochraně života a zdraví samotných zaměstnanců a třetích osob. Zaměstnavatel nemůže postupovat při kontrole naprosto libovolně, ale kontrola musí být vždy *„přiměřená cíli a musí narušovat soukromí zaměstnance jen v rozsahu, který je nezbytný k výkonu práce, případně k ochraně majetku zaměstnavatele.“*²²⁹ Sledováním zaměstnanců tak v žádném případě nesmí docházet k nepřiměřenému zásahu do soukromí zaměstnanců.²³⁰

²²⁸ srov. § 302 zákoníku práce či § 248 odst. 2 zákoníku práce

²²⁹ Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012

²³⁰ ŠTEFKO MARTIN in BĚLINA, MIROSLAV, DRÁPAL, LJUBOMÍR A KOL. *Zákoník práce. Komentář*. 2. vydání. Praha : C. H. Beck, 2015, s. 1243

Autor považuje toto ustanovení za poměrně problematické a to z několika důvodů. Prvním z nich je výklad toho, co znamená závažný důvod spočívající v povaze činnosti zaměstnavatele. Dle názoru autora nelze tento důvod spatřovat pouze ve zvlášť nebezpečných provozech, jako jsou např. jaderné elektrárny. Problematické také je, že osobou, která rozhoduje o zavedení sledování je vždy zaměstnavatel bez jakékoliv konzultace či projednání, byť i s odborovou organizací. Na zaměstnavateli tedy leží břemeno, aby důkladně zvážil nejen subsidiaritu, ale také proporcionalitu případného zásahu do soukromí zaměstnanců, což pro ně bezpochyby představuje velmi složitý úkol, který je bez znalosti této problematiky prakticky nemožné spolehlivě vyřešit. Autor je poměrně skeptický k aplikační praxi a je přesvědčen, že mnoho zaměstnavatelů výše uvedenou proceduru odmítá podstoupit a místo toho rovnou např. nainstalují kamerový systém.

Další problém tohoto ustanovení doposud představoval fakt, že zákon o inspekci práce neobsahoval skutkovou podstatu přestupku proti výše uvedenému ustanovení zákoníku práce.²³¹ Inspektoráty práce v případě, že došly k závěru, že zaměstnavatel porušuje předpisy týkající se ochrany osobních údajů, daný případ předávaly UOOU. Problémem tohoto postupu bylo, že ne všechno sledování zaměstnanců bylo zpracováním osobních údajů, a proto se na něj nemusel vztahovat Zákon. Příkladem budiž sledování zaměstnanců online kamerovým systémem bez pořizování záznamu. V dnešní době může zaměstnavatel pomocí chytrého telefonu soustavně sledovat své zaměstnance ze všech koutů světa. Takové zpracování může být daleko více invazivní než instalace kamerového systému se záznamem, který zaměstnavatel prohlíží až za předpokladu, že nastane nějaká neočekávaná situace, např. pracovní úraz zaměstnance. V prvním případě zaměstnavatel sice jednal v rozporu se zákoníkem práce, ale nemohla mu být za takové jednání udělena sankce, odhlédneme-li od civilněprávní možnosti ochrany fyzických osob. V druhém případě UOOU zkoumalo, zda zaměstnavatel dodržuje ustanovení Zákona a v případě, že ne, tak mu mohl udělit sankci za spáchaný přestupek.

Na výše uvedenou situaci, kdy inspekce práce sice mohla kontrolovat dodržování § 316 zákoníku práce, ale nemohla při zjištění porušení uložit sankční

²³¹ Zákon č. 251/2005 Sb., o inspekci práce, ve znění pozdějších předpisů

opatření, upozorňoval i Veřejný ochránce práv již ve své souhrnné zprávě za rok 2013.^{232 233} Na to reagovala vláda, která vypracovala návrh zákona, kterým se mění zákon o zaměstnanosti a další související zákony, mezi nimiž právě i zákon o inspekci práce, která byla schválena a nabyla účinnosti dne 29. 7. 2017.²³⁴

Vláda v důvodové zprávě uvedla, že cílem návrhu zákona je zlepšením kontrolních mechanismů, tedy zavedení možnosti inspekce práce udělit finanční postih, který bude obsahovat preventivní i represivní složku, čímž nejen, že se zvýší efektivita a účinnost kontroly, ale také dojde ke zvýšení ochrany soukromí a osobních práv zaměstnanců. Novela také zefektivňuje spolupráci mezi UOOU a orgány inspekce práce, když UOOU budou předávány pouze ty podněty, které budou spadat do jeho působnosti.²³⁵

Tato novela nezakládá nové ani nemění již existující způsoby zpracování osobních údajů. V daném případě se jedná pouze o zavedení zvláštních skutkových podstat přestupků za porušení již existujícího ustanovení § 316 zákoníku práce do zákona o inspekci práce.²³⁶

Podle této novely se přestupku na úseku ochrany soukromí a osobních práv zaměstnanců dopustí fyzická osoba či právnická nebo podnikající fyzická osoba jako zaměstnavatel, pokud (a) naruší soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele některým ze způsobů uvedených v § 316 odst. 2 zákoníku práce; (b) neinformuje zaměstnance o rozsahu kontroly

²³² pozn. Inspekce práce mohla pouze uložit zaměstnavateli opatření k nápravě či podat podnět k UOOU, přičemž pochybení zaměstnavatele inspekce práce pouze uvedla do protokolu o provedené kontrole.

²³³ srov. VEŘEJNÝ OCHRÁNCE PRÁV *Souhrnná zpráva o činnosti veřejného ochránce práv 2013*. Dostupná z https://www.ochrance.cz/fileadmin/user_upload/zpravy_pro_poslaneckou_snemovnu/Souhrn_na-zprava_2013_PDF_A.pdf [cit. 10. 8. 2017]

²³⁴ PSP *Sněmovní tisk č. 911/0 - Vládní návrh zákona, kterým se mění zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a další související zákony*. Dostupný z <http://www.psp.cz/sqw/text/tiskt.sqw?O=7&CT=911&CT1=0> [cit. 10. 8. 2017]

²³⁵ srov. Důvodová zpráva k zákonu č. 206/2017 Sb., kterým se mění zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a další související zákony. Dostupná z <http://www.psp.cz/sqw/text/tiskt.sqw?O=7&CT=911&CT1=0#prilohy> [cit. 10. 8. 2017]

²³⁶ Tamtéž

a o způsobech jejího provádění podle § 316 odst. 3 zákoníku práce, nebo (c) v rozporu s § 316 odst. 4 zákoníku práce vyžaduje od zaměstnance informace, které bezprostředně nesouvisejí s výkonem práce a se základním pracovněprávním vztahem. Za takový přestupek může inspektorát práce uložit pokutu až do výše 1 milionu Kč, a to bez ohledu na to, zda je zaměstnavatelem fyzická osoba či osoba podnikající.

Autor považuje doplnění skutkových podstat výše uvedených přestupků do zákona o inspekci práce za pozitivní, ale zatím je brzo na jakékoli hodnocení dopadů na aplikační praxi.

Nelze opomenout, že sledování zaměstnanců je obvykle ze své povahy zpracováním osobních údajů zaměstnanců, a tak je potřeba vzít v potaz i některá ustanovení Zákona.²³⁷ S ohledem na to, že § 316 odst. 2 zákoníku práce se považuje za kogentní ustanovení, tak není možné z uvedeného rámce sledování zaměstnance vybočit, a to ani v případě, že by samotný zaměstnanec s tím souhlasil.²³⁸ Z toho vyplývá, že právním titulem pro takové zpracování osobních údajů nemůže být souhlas zaměstnanců podle § 5 odst. 2 Zákona.²³⁹

Předmětem této kapitoly je přiblížit některé případy monitoringu zaměstnanců, s nimiž je možné se v aplikační praxi setkat. Pozornost bude věnována zejména sledování aktivity zaměstnanců na internetu, monitorování e-mailové korespondence a služebních telefonů zaměstnanců, kontrole služebních automobilů a také kamerovým systémům na pracovišti.

6.1 Sledování aktivity zaměstnanců na internetu

Jednou z možností kontroly zaměstnanců představuje sledování jejich aktivity na internetu. Zaměstnavatelé mnohdy kontrolují zaměstnance, zda si svoji pracovní dobu nekrátí „brouzdáním“ po internetu, užíváním sociálních sítí, hraním online her nebo dokonce sledováním různých seriálů či filmů, a to zejména v případě, že je to

²³⁷ pozn. zejména základní zásady ochrany osobních údajů či povinnosti správce

²³⁸ srov. náleží Ústavního soudu ze dne 12. 3. 2008, sp. zn. Pl. ÚS 83/06

²³⁹ pozn. v případě sledování zaměstnanců bude právním titulem nejčastěji § 5 odst. 2 písm. e) – ochrana práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby

na úkor jejich pracovní výkonnosti. Dalším důvodem samozřejmě může být technická ochrana výpočetní techniky zaměstnavatele před nežádoucími škodlivými programy, zejména viry.

V dnešní době je otázkou, zda by zaměstnavatelé využívání internetu k soukromým aktivitám v rámci pracovní doby měli striktně zakazovat. To ovšem neznamená, že by si zaměstnanci mohli dělat, co uznají za vhodné a vykonávat práci v omezeném rozsahu. Autor se domnívá, že zaměstnavatelé by měli předcházet tomu, aby byli nuceni přistupovat k samotné kontrole tím, že rozumně nastaví pravidla přístupu na internet ve vnitřním předpisu. Takový vnitřní předpis by také mohl obsahovat obecné vymezení zakázaných webových stránek a dobu, po kterou může zaměstnanec využívat služební počítač k soukromým účelům.²⁴⁰ Striktní zakázání přístupu na internet nejen, že by nezvýšilo pracovní výkonnost zaměstnanců, ale mohlo by vést k tomu, že by zaměstnanci své záležitosti stejně řešili pomocí svých mobilních telefonů.

Za předpokladu, že se zaměstnavatel dozvěděl, že zaměstnanci pravděpodobně nevhodně nakládají s prostředky zaměstnavatele či s jejich pracovní dobou, tak může „*přistoupit ke zpracování jejich osobních údajů v rozsahu datum, hodina a délka přístupů na webové stránky a míra aktivity na nich.*“²⁴¹

Nejvyšší soud se problematice monitorování zaměstnanců věnoval již v několika rozhodnutích, z nichž největší rozruch vzbudilo rozhodnutí z roku 2012.²⁴² V daném případě se soudy zabývaly otázkou (ne)platnosti okamžitého zrušení pracovního poměru zaměstnavatelem pro zvlášť hrubé porušení povinností zaměstnance podle § 55 odst. 1 písm. b) zákoníku práce. Zaměstnavatel zvlášť hrubé porušení povinností spatřoval v tom, že zaměstnanec v průběhu jednoho měsíce strávil více než 100 hodin své pracovní doby prohlížením internetových stránek, vyřizováním soukromých e-mailů a hraním online her. Hlavním argumentem

²⁴⁰ pozn. s tím souvisí i možnost nainstalovat software, který neumožňuje zaměstnancům přístup na předem stanovené webové stránky

²⁴¹ MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 405. ISBN 978-80-7478-139-1.

²⁴² Rozsudek Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011

zaměstnanec bylo, že jednak užití počítače pro soukromé účely nebylo na úkor plnění pracovních povinností, za druhé intenzita takového porušení povinnosti nedosáhla intenzity zvláště hrubého porušení a konečně za třetí zaměstnavatel sledoval zaměstnance tajně v rozporu s § 316 odst. 2 zákoníku práce, a tak takový důkaz je nepřipustný.

Soudy dospěly k tomu, že vzhledem k celkové době, kterou zaměstnanec strávil uvedenou činností (více než 60 % své pracovní doby), tak se opravdu jedná o zvláště hrubé porušení povinností. K (ne)připustnosti důkazu odvolací soud uvedl, že zaměstnavatel sledoval pouze pohyb zaměstnance na internetu, a nikoliv samotný obsah navštívených internetových stránek, a tak takový důkaz připustil.²⁴³ S tím souhlasil i Nejvyšší soud, který v daném případě nadřadil ochranu majetku zaměstnavatele nad soukromí zaměstnance.²⁴⁴

Dle názoru autora v daném případě převážil vysoký rozsah strávený mimopracovními aktivitami nad dalšími otázkami. V daném případě soudům práci ulehčil i postup zaměstnavatele, který aktivně stanovil pravidla ve vnitřním předpisu a monitoroval pouze dobu strávenou mimopracovní aktivitou a nikoli samotný obsah.

Nelze ovšem tvrdit, že tato problematika je otázkou jednoznačnou a konečně vyřešenou. Zajímavé by jistě bylo, kdyby daný rozsah strávený mimopracovní aktivitou byl minimální. V takovém případě by soudy možná nepovažovaly intenzitu takového porušení za zvláště hrubou. Je také možné, že by takovou mimopracovní aktivitu zaměstnanec soudy posoudily jako předstíranou práci, která dle judikatury představuje útok na majetek zaměstnance (pokus získat mzdu za práci v době, kdy zaměstnanec nepracuje).²⁴⁵ Vzhledem k tomu, že soudy nastavily velmi přísnou linii

²⁴³ „Je tedy zřejmé, že prováděná kontrola směřovala toliko k ochraně majetku zaměstnavatele. O soukromí zaměstnance (o jeho osobnosti) jistě vypovídá i údaj o tom, které internetové stránky sleduje, avšak podstatou kontroly nebylo toto zjištění, nýbrž pouze zjištění, zda zaměstnanec (i žalobce) sledoval takové internetové stránky, které s výkonem jeho práce nesouvisely.“

²⁴⁴ pozn. zaměstnanec se poté obrátil na Ústavní soud, který ústavní stížnost usnesením odmítl jako zjevně neopodstatněnou (sp. zn. I. ÚS 3933/2012)

²⁴⁵ srov. rozsudek Nejvyššího soudu ze dne 17. 10. 2012, sp. zn. 21 Cdo 2596/2011

týkající se útoků zaměstnanců na majetek zaměstnavatele, tak by v takovém případě okamžité zrušení pracovního poměru mohlo být namístě.²⁴⁶

Autor se i přesto domnívá, že soudy a vlastně také zaměstnavatelé by měli intenzitu takového porušení posuzovat v každém jednotlivém případě k přihlédnutím zejména k době strávené mimopracovními aktivitami a k plnění pracovních úkolů zaměstnancem zcela individuálně. Autor je toho názoru, že i na pracovišti by měl mít zaměstnanec možnost, byť i v minimálním rozsahu, vyřídit si některé své soukromé záležitosti, protože mnohdy mimo pracovní dobu již taková možnost není.

Na výše uvedené rozhodnutí navázal Nejvyšší soud rozhodnutím z roku 2014.²⁴⁷ V daném případě zaměstnavatel se zaměstnancem rozvázal pracovní poměr výpovědí pro soustavné méně závažné porušování pracovních povinností. Zaměstnavatel totiž napočítal zaměstnanci tři různá porušení – šlo o používání služebního počítače pro soukromé účely (vyhledávání informací na internetu), používání služebního telefonu pro soukromé účely (84 hovorů) a do třetice pozdní příchod na pracoviště (20 minut). Zaměstnanec se rozhodl nenechat situaci být a podal proti zaměstnavateli žalobu k soudu. Ve sporu šlo mimo jiné o to, zda zaměstnavatel kontrolou soukromých hovorů zaměstnance narušil zaměstnancova práva a zda tedy šlo o nepřípustný důkaz.

Obecné soudy rozhodovaly v tomto případě, na rozdíl od výše uvedeného případu, jako na houpačce. U soudu prvního stupně uspěl zaměstnanec, odvolací soud dal naopak za pravdu zaměstnavateli. Konečnou instancí tak byl až Nejvyšší soud, který se přiklonil na stranu zaměstnavatele. Nejvyšší soud znovu potvrdil, že pokud kontrola nezjišťovala obsah prohlížených stránek a soukromých telefonátů, ale jen to, zda zaměstnanec respektuje zákaz používání počítače a telefonu pro soukromé účely, šlo o kontrolu přiměřenou a přípustnou.

Soudům ve výše uvedených sporech lze vytknout, že na danou problematiku nenahlédly z pohledu Zákona. Nelze opomenout fakt, že UOOU dlouhodobě zastává

²⁴⁶ srov. rozsudek Nejvyššího soudu ze dne 21. 1. 2014, sp. zn. 21 Cdo 1496/2013 a rozsudek Nejvyššího soudu ze dne 19. 7. 2016, sp. zn. 21 Cdo 2590/2015

²⁴⁷ Rozsudek Nejvyššího soudu ze dne 7. 8. 2014, sp. zn. 21 Cdo 747/2013

stanovisko, že zaměstnavatel zásadně není oprávněn monitorovat obsah soukromé komunikace svých zaměstnanců za žádných okolností, kromě zcela výjimečných případů, kdy je zřejmé, že se soukromá zpráva zaměstnance týká výkonu práce zaměstnance. Otázkou je, zda výše uvedené lze vztáhnout i na sledování „pohybu“ zaměstnance po internetu. V opačném případě, tak může dojít k paradoxní situaci, kdy zaměstnavatel uspěje ve sporu se zaměstnancem, protože podle soudu neporušil právní předpisy, ale zároveň bude ze strany UOOU pokutován za naprosto totožné jednání.

6.2 Monitorování e-mailové korespondence

Se sledováním zaměstnanců nepochybně souvisí také problematika kontroly elektronické pošty a jiné elektronické komunikace zaměstnanců. Co se elektronické formy právního jednání týká, tak dle § 562 odst. 1 občanského zákoníku se považují za písemnosti a samozřejmě se na ně vztahuje takové listovní tajemství dle článku 13 Listiny.^{248 249}

Vzhledem k tomu, že zaměstnavatel v žádném případě nesmí zasahovat do plně soukromých e-mailových adres svých zaměstnanců, obvykle založených bezplatně u různých poskytovatelů, tak tato podkapitola bude věnována e-mailovým adresám, které mají návaznost na výkon závislé práce.²⁵⁰

K této problematice se také vyjádřil UOOU ve stanovisku č. 2/2009, podle něj se rozlišují e-mailové adresy patřící zaměstnavateli podle toho, jakou podobu daná adresa má.²⁵¹

²⁴⁸ „Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby.“ (§ 562 odst. 1 občanského zákoníku)

²⁴⁹ „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. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.“ (článek 13 Listiny)

²⁵⁰ pozn. bezplatně založená e-mailová adresa bývá označována jako tzv. „freemail“

²⁵¹ Stanovisko UOOU č. 2/2009 - Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. Dostupné z https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=22563 [cit. 2. 7. 2017]

V případě, že je e-mailová adresa složena ze jména a příjmení zaměstnance (např. jakub.lejsek@zamestnavatel.cz), tak se tato adresa považuje dokonce za osobní údaj a e-mail na ni doručený za soukromou poštu. Naproti tomu věcně konstruovaná e-mailová adresa (např. office@zamestnavatel.cz) je i v případě, že ji užívá jediný zaměstnanec považována za úřední elektronickou adresu.²⁵²

Zaměstnavatel není oprávněn sledovat či jinak zpracovávat obsah korespondence svých zaměstnanců, ale je oprávněn sledovat počet došlých a odeslaných zpráv, a to zejména za předpokladu podezření ze zneužití pracovních prostředků i hlavičku e-mailu či jeho předmět.²⁵³

UOOU dále ve výše uvedeném stanovisku připouští možnost zaměstnavatele v zájmu ochrany svých práv ve výjimečných případech otevřít „soukromý“ email (e-mail se jménem a příjmením zaměstnance, ale s doménou zaměstnavatele) za předpokladu, že se jedná o pracovní e-mail.²⁵⁴ Za výjimečný případ by se mohla považovat situace, kdy je zaměstnanec dlouhodobě nemocný a zaměstnavatel by v případě neodpovědění mohl např. přijít o určité zakázky či klienty, čímž by jistě došlo ke škodě na jeho právech. Zjistí-li zaměstnavatel, že otevřený e-mail, doručený na soukromou e-mailovou adresu je opravdu soukromé povahy, tak není oprávněn takový e-mail dočíst a měl by ho neprodleně zavřít.²⁵⁵

Zaměstnavatelům lze jistě doporučit, aby si ve svých vnitřních předpisech stanovili a zaměstnance s tím řádně seznámili, zda zaměstnanci mohou, případně jakým způsobem a v jakém rozsahu užívat pracovní e-mail pro soukromé účely. Vhodné je jistě i nastavit pravidla pro e-mailové adresy zaměstnanců, kteří se ocitli mimo pracoviště např. z důvodu dovolené. Vhodným řešením se zdá být nastavení automatické odpovědi, kde se odesílateli sdělí, že daný zaměstnanec se nachází

²⁵² Tamtéž

²⁵³ Tamtéž

²⁵⁴ pozn. UOOU tímto trochu popřel samotné dělení pracovních e-mailových adres na soukromé a úřední, kdy umožňuje zaměstnavateli v určitých případech nahlédnout i do soukromé e-mailové adresy.

²⁵⁵ pozn. v opačném případě by se mohlo jednat o porušení listovního tajemství

mimo své pracoviště a že v případě potřeby je možné kontaktovat jiného zaměstnance na uvedené e-mailové adrese.

Ke sledování e-mailové komunikace a obecně ke sledování pohybu zaměstnance na internetu se vyjádřil i ESLP, a to ve známém rozsudku ve věci *Barbulescu proti Rumunsku*.²⁵⁶

Zaměstnanec (pan Barbulescu) si na pokyn svého zaměstnavatele zřídil účet v programu Yahoo Messenger za účelem efektivnější komunikace se zákazníky. Následně byl informován o tom, že jeho komunikace byla monitorována a že porušil interní pravidla zaměstnavatele tím, že v pracovní době využíval internet k soukromým účelům (např. soukromé zprávy se snoubenkou a bratrem). Zaměstnavatel na základě toho ukončil se zaměstnancem pracovní poměr.

Zaměstnanec se obrátil na soud, kde se domáhal určení neplatnosti výpovědi, což odůvodnil tím, že podklady pro zrušení pracovního poměru byly získány v rozporu s jeho právem na ochranu listovního tajemství a soukromého života. Před rumunskými soudy zaměstnanec neuspěl, a tak se obrátil na ESLP, kde namítal porušení článku 8 Evropské úmluvy (právo na respektování soukromého a rodinného života).

ESLP usoudil, že objektivně došlo k zásahu do soukromí zaměstnance, a tak přešel k posouzení, zda rumunské soudy vyváženě posoudily právo zaměstnance na soukromí a oprávněné zájmy zaměstnavatele. ESLP nakonec dospěl k tomu, že zaměstnavatelé samozřejmě mohou kontrolovat své zaměstnance, zda pracují a v daném případě samotná kontrola byla jen velmi omezená a po velmi krátkou dobu, a proto soud dospěl k tomu, že čl. 8 Evropské úmluvy nebyl porušen.

Přestože tento rozsudek vzbudil ve sdělovacích prostředcích poměrně velký ohlas, tak se nejedná o nějaký velký zlom v nastolené judikatuře a rozhodně ho nelze vykládat způsobem, že zaměstnavatel může plošně sledovat veškerou

²⁵⁶ Rozsudek ESLP ze dne 12. 1. 2016, stížnost č. 61496/08

korespondenci zaměstnance. ESLP dospěl „pouze“ k tomu, že za určitých okolností je legitimní kontrolovat využití internetu ze strany svých zaměstnanců.²⁵⁷

6.3 Monitorování služebních telefonů

S monitorováním e-mailové komunikace částečně souvisí i kontrola využívání služebních telefonů zaměstnanců. Zaměstnavatelé velmi často poskytují svým zaměstnancům služební mobilní telefony, které zaměstnanci mohou často využívat i pro soukromé účely. V literatuře se mnohdy objevuje řešení pro odlišení služebních hovorů od soukromých pomocí určité předvolby, aby soukromé hovory mohly být samostatně účtovány.²⁵⁸ Tento postup již, dle názoru autora, nemá opodstatnění, a to z důvodu masového rozšíření tzv. neomezených tarifů. Motivem případné kontroly využívání služebního telefonu by tedy nebyla úspora za provolané minuty, ale kontrola, zda zaměstnanec řádně využívá svoji pracovní dobu pracovní činností.

Pro sledování hovorů zaměstnanců platí obdobné, co pro e-mailovou komunikaci a zaměstnavatel je povinen ctít tajemství obsahu podávaných zpráv a soukromí zaměstnance.²⁵⁹ Podle ESLP se „*na telefonní hovory z firemních prostor podle předchozí judikatury soudu zcela jasně vztahují pojmy „soukromý život“ a „korespondence“ uvedené v čl. 8 odst. 1 Evropské úmluvy.*“²⁶⁰

Zaměstnavatel tedy není oprávněn sledovat (odposlouchávat) hovory zaměstnanců, a to i za předpokladu, že se jedná o soukromé rozhovory či vyřizování čistě osobních záležitostí ze služebního telefonu a v rámci pracovní doby.

²⁵⁷ NONNEMANN, FRANTIŠEK *Sledování aktivity zaměstnance na internetu ve světle aktuální judikatury Evropského soudu pro lidská práva*. In: Epravo.cz [online]. Dostupné z <https://www.epravo.cz/top/clanky/sledovani-aktivity-zamestnance-na-internetu-ve-svetle-aktualni-%20judikatury-evropskeho-soudu-pro-lidska-prava-100316.html> [cit. 2. 7. 2017]

²⁵⁸ JANEČKOVÁ, EVA, BARTÍK, VÁCLAV *Ochrana osobních údajů v pracovním právu (Otázky a odpovědi)*. Praha: Wolters Kluwer, 2016, s. 88-90. ISBN 978-80-7552-145-3.

²⁵⁹ Čl. 13 Listiny

²⁶⁰ srov. rozsudek ESLP ze dne 3. 4. 2007, Copland proti Spojenému království, stížnost č. 62617/00

6.4 Kontrola služebních automobilů

Mnoho zaměstnanců vykonává svoji práci „mobilně“, a tak k jejímu výkonu nezbytně potřebují automobil. Typicky se jedná o kurýry, obchodní zástupce či profesionální řidiče. S ohledem na to, že náklady na provoz a cena vozidla je nesrovnatelně vyšší než obvyklé pracovní prostředky, tak se zaměstnavatelé uchylují ke kontrole nejen efektivity práce zaměstnanců, ale i k ochraně svého majetku pomocí GPS lokalizátorů.

GPS lokalizátory jsou schopny určit přesnou polohu vozidla a umožnit její sledování online. Tyto systémy jsou dále schopny vyhodnotit náklady na provoz automobilu, sledovat průběh jízdy či dodržování dopravních předpisů a automaticky generovat podrobnou knihu jízd.²⁶¹

Jak již bylo výše uvedeno, tak zaměstnavatel nesmí bez závažného důvodu kontrolovat své zaměstnance a jakákoliv kontrola musí být přiměřená a nesmí narušovat soukromí zaměstnance víc než v nezbytně nutné míře. Za závažný důvod lze jistě považovat převoz finančních prostředků, převoz zásilek kurýrem či ochranu proti krádeži v oblasti, kde ke krádežím dochází. Zaměstnavatel by v takovém případě měl zaměstnance informovat o instalovaném monitorovacím zařízení a náležitě ho seznámit s pravidly jeho používání.²⁶²

UOOU se ve své aplikační praxi setkal i s dalším „bohulibým“ důvodem zavedení GPS lokalizátorů, a to za účelem kontroly a optimalizace doručovacích okrsků (optimalizace tras).²⁶³ V daném případě správcem byla Česká pošta, s.p. („**Česká pošta**“), která nejen že sledovala pohyb služebních vozidel, ale také jednotlivým zaměstnancům „rozdala“ GPS lokalizátory a sledovala jejich pohyb. V daném případě se Česká pošta dopustila správního deliktu (v současné terminologii přestupku), jelikož zpracovávala osobní údaje bez souhlasu svých

²⁶¹ UOOU *Ochrana osobních údajů na pracovišti* ISBN 978-80-210-6819-3. Dostupné z https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691 [cit. 6. 7. 2017]

²⁶² srov. KADLECOVÁ TEREZA, *GPS ve služebních vozidlech aneb malý čip = velká komplikace?* Praktická personalistika, Olomouc: ANAG č. 3-4/2015, s. 9 a násl. ISSN 2336-5072

²⁶³ Rozhodnutí UOOU ze dne 3. 7. 2013, č.j. UOOU-00237/13-38

zaměstnanců.²⁶⁴ UOOU dále upozorňoval na to, že Česká pošta přesahovala stanovený účel zpracování a nad jeho rámec zpracovávala osobní údaje svých zaměstnanců po nepřiměřenou dobu. Mimo to, také nebylo nezbytné, dle UOOU, zpracovávat osobní údaje zaměstnanců po celou jejich pracovní dobu.

Autor této práce se domnívá, že stanovený účel – optimalizace tras i přes výše uvedené rozhodnutí UOOU může obstát, a to i bez souhlasu subjektu údajů podle § 5 odst. 2 Zákona. Právním titulem v takovém případě by mohl být § 5 odst. 2 písm. e) Zákona, tedy pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo dotčené osoby. Je nutné ale zmínit, že takové zpracování by muselo být jen v nezbytně nutném rozsahu, aby nedocházelo k zásahu do soukromého a osobního života zaměstnanců. Ochranu práv a právem chráněných zájmů autor spatřuje v udržení a zajištění kvality poskytovaných služeb, jelikož v případě, že by poštovní služba se nesnažila zefektivnit a zkvalitnit své služby, tak by ji mohla předstihnout konkurence.

V případě, že zaměstnanci mohou užívat svěřený automobil i k soukromým cestám, tak zaměstnanec musí mít možnost monitorovací zařízení vypnout či přepnout do režimu soukromých cest, aby zaměstnavatel neměl možnost sledovat pohyb vozidla.²⁶⁵ Otázkou je, zda taková monitorovací zařízení opravdu existují. Některé z nabízených totiž mají přepínací systém na soukromé cesty, jejichž evidence se zaměstnavateli nezasílá, ale v případě nutnosti lze i tato data ze zařízení získat.

6.5 Kamerové systémy

V dnešní době zřejmě nejrozšířenějším způsobem sledování osob představují kamerové systémy. V souvislosti s technologickým rozvojem se kamerové systémy začali objevovat nejen na veřejně přístupných místech, ale také třeba na pracovištích či v soukromých prostorách. Vzhledem k jejich rozšířenosti dnes již nelze mluvit

²⁶⁴ pozn. porušila povinnost stanovenou v § 5 odst. 2 Zákona, tedy povinnost zpracovávat osobní údaje se souhlasem subjektů údajů, aniž by naplnila některou z výjimek stanovených v § 5 odst. 2 písm. a) až g) Zákona

²⁶⁵ pozn. na základě souhlasu (dohody) zaměstnavatele § 316 odst. 1 zákoníku práce

o vzrůstajícím fenoménu, ale spíše o realitě všedního dne, a to zejména ve větších městech.

Kamerové systémy jsou obecně instalovány za různými účely, z nichž zřejmě nejčastější představuje ochrana jednotlivců, ochrana majetku, veřejný zájem či odhalování a prevence trestné činnosti.²⁶⁶

Co se kamerových systémů na pracovišti týká, tak se zde opět prolíná úprava Zákona a zákoníku práce. Z tohoto pohledu je důležité zmínit, že ne všechny kamerové systémy spadají do působnosti Zákona. V případě, že daný kamerový systém pouze monitoruje sledované místo a není pořizován záznam, tak se nejedná o zpracování osobních údajů ve smyslu Zákona.²⁶⁷ Další otázkou je, zda se vůbec jedná o osobní údaj a tedy zda je z pořizovaného záznamu možné identifikovat jednotlivce. Pakliže by daný záznam neumožňoval identifikaci jednotlivce, tak by se opět nejednalo o zpracování osobních údajů. O identifikovatelnosti jednotlivce jistě nebude pochyb, pokud bude zaznamenán jeho obličej či jiné charakteristické rozpoznávací znaky.²⁶⁸

I za předpokladu, že kamerový systém nebude podléhat Zákonu, i tak může velmi negativně zasahovat do soukromí jednotlivých osob, a to i v případě instalace pouhé makety. Lze tedy doporučit každému, aby předtím než nainstaluje kamerové zařízení či jeho napodobeninu, pečlivě zvážil nejen Zákon a jeho ustanovení, ale aby se zamyslel nad tím, zda nenarušuje soukromí ostatních jednotlivců a jak by se mu líbilo, kdyby byl v opačné pozici.²⁶⁹

²⁶⁶ Stanovisko WP 29 č. 4/2004 Ke zpracování osobních údajů prostředky kamerového sledování. Dostupné z https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=22427 [cit. 6. 7. 2017]

²⁶⁷ srov. UOOU Stanovisko č. 1/2006 – *Provozování kamerového systému z hlediska zákona o ochraně osobních údajů*. Dostupné z https://www.uoou.cz/files/stanovisko_2006_1.pdf [cit. 6. 7. 2017]

²⁶⁸ Tamtéž

²⁶⁹ pozn. v tomto případě je vhodné zvážit již zmíněnou zásadu – „*nečiň jinému to, co nechceš, aby on činil tobě*“

Jak již bylo uvozeno, tak při zavádění kamerových systémů na pracoviště, nepostačí jen ustanovení Zákona, ale zaměstnavatel musí přihlídnout také k již několikrát zmiňovanému, klíčovému § 316 zákoníku práce.

Zaměstnavatel by, dle názoru autora, měl postupovat co nejohleduplněji a přistupovat k zavedení kamerového systému jako prostředku *ultima ratio*, tedy až v případě, že jiné, méně invazivní prostředky, se ukáží jako neúčinné. K ochraně majetku zaměstnavatele mnohdy postačí např. zavedení zabezpečovacího systému namísto instalace kamerového systému. V případě nadměrného sledování, mohou zaměstnanci cítit ze strany zaměstnavatele nedůvěru a v takovém pracovním prostředí se jim může pracovat velmi špatně.²⁷⁰ Navíc ne všichni zaměstnanci se dokáží pod tíhou tlaku „vybičovat“ k lepším pracovním výkonům, a naopak může dojít v důsledku obav případného postihu ke snížení jejich pracovní výkonnosti.

Pakliže zaměstnavatel dospěje k tomu, že je nezbytné zavést kamerový systém, tak by měl vzít na vědomí, že tím může narušit soukromí zaměstnance. Takové narušení však zaměstnavatel nemůže „obejít“ tím, že požádá zaměstnance o jeho souhlas jako právní titul pro dané zpracování, protože souhlasem by se zaměstnanec předem vzdával svého práva na soukromí.²⁷¹

Kamerové systémy může zaměstnavatel na pracovišti zavést jen za předpokladu, že zde existuje důvod spočívající ve zvláštní povaze jeho činnosti.²⁷² Takovou zvláštní povahu lze spatřovat např. v pracovišti, kde se pracuje s vyšší finanční hotovostí nebo kde je zvýšené nebezpečí vzniku pracovního úrazu.

I za předpokladu, že zaměstnavatel splní výše uvedené kritérium, tak to neznamená, že by mohl monitorovat pracoviště a v návaznosti na to i své zaměstnance naprosto neomezeně. Zaměstnavatel by měl respektovat právo zaměstnance na soukromí, a proto by neměl monitorovat prostory, které slouží zaměstnancům pro soukromé účely nebo nejsou určeny k plnění pracovních

²⁷⁰ BARTÍK, VÁCLAV, JANEČKOVÁ, EVA *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 3. vydání Praha: Linde, 2013, s. 143 a násl. ISBN 978-80-86131-96-2

²⁷¹ JANEČKOVÁ, EVA, BARTÍK, VÁCLAV *Ochrana osobních údajů v pracovním právu (Otázky a odpovědi)*. Praha: Wolters Kluwer, 2016, s. 132-133. ISBN 978-80-7552-145-3.

²⁷² § 316 odst. 2 zákoníku práce

povinností jako např. toalety, sprchy, šatny atd.²⁷³ Zaměstnavatel by také měl zvážit počet a rozmístění kamer tak, aby byl monitoring směřován na jeho majetek a ne přímo na osobu zaměstnance.²⁷⁴

Zaměstnavatel je podle Zákona samozřejmě povinen informovat své zaměstnance o takovém zpracování a o jejich právech s tím souvisejícím.²⁷⁵ Samotná cedulka s piktogramem kamery pro dotčené zaměstnance nepředstavuje dostatečnou informaci. Takovou cedulkou je ale nezbytné označit monitorovaný prostor v případě, že je určen i pro další osoby např. klienty. V praxi se lze setkat s různými cedulkami, ale většina z nich obsahuje informace neúplné či naprosto nedostatečné. Takové označení monitorovaných prostor by mělo obsahovat alespoň piktogram kamery, informaci, že daný prostor je monitorován kamerovým zařízením se záznamem, identifikaci správce a odkaz na osobu či místo, kde je možné získat o kamerovém systému další informace.²⁷⁶

²⁷³ Stanovisko WP 29 č. 4/2004 Ke zpracování osobních údajů prostředky kamerového sledování. Dostupné z https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=2427 [cit. 6. 7. 2017]

²⁷⁴ Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012

²⁷⁵ VIDRNA, JAN, KOUDELKA ZDENĚK *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců*. 1 vydání. Praha : C. H. Beck, 2013, s. 86 a násl.

²⁷⁶ UOOU *Provozování kamerových systémů: Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů*. ISBN 978-80-210-6017-3 Dostupné z https://www.uoou.cz/files/metodika_provozovani_kamerovych_systemu.pdf [cit. 7. 7. 2017]

Závěr

Cílem autora nebylo kazuisticky postihnout veškerá zpracování osobních údajů, ke kterým může v pracovněprávních vztazích dojít. Splnit takový cíl by se dalo považovat za sisyfovský úkol a s ohledem na velmi rychlý vývoj informačních technologií by v takovém případě práce zůstala, pakliže by se opravdu podařilo postihnout veškeré možné zpracování, jen velmi krátce aktuální. V takovém případě by si však práce zasloužila daleko větší pozornost než pouhé zpracování v rámci diplomové práce.

Tato oblast představuje velmi širokou problematiku a z toho důvodu si autor vytyčil za cíl „pouhé“ přiblížení obecné teorie s její následnou aplikací na konkrétní příklady. I přes to, že si autor byl plně vědom, že daná materie je velmi rozsáhlá, v průběhu psaní se jeho názor ještě více prohloubil. Na tuto problematiku je totiž navázáno mnoho dalších právních předpisů a možností sledovat své zaměstnance je nesčetně mnoho.

O aktuálnosti tématu hovoří i to, že řada autorů se touto problematikou zabývá. Nutno dodat, že většina odborné literatury se věnuje jen jednotlivým aspektům zpracování a neposkytují, až na výjimky, ucelený náhled na celou problematiku.

Ochrana osobních údajů je integrálně spjata s ústavní zárukou nedotknutelnosti člověka a jeho soukromí. Z tohoto důvodu bylo velmi důležité vymežit, co vlastně soukromí znamená a že i zaměstnanec vykonávající závislou práci má právo na soukromí, a to i na samotném pracovišti.

Poté následoval krátký exkurz do vývoje této materie na mezinárodním, regionálním a národním poli, který ukazuje, že daná problematika je sice relativně mladou právní disciplínou, ale o to více aktuální a dynamickou. Ačkoli mnozí lidé považují tuto problematiku za „výdobytek“ společnosti, je potřeba se s ní velmi pečlivě zabývat a nebrat ji jen jako okrajovou záležitost.

Na to navazuje popis některých klíčových pojmů s následným vymezením důležitých práv a povinností subjektů v pracovněprávních vztazích. Nejzajímavější část této práce avšak tvoří kapitoly týkající se zpracování osobních údajů

v jednotlivých fázích pracovního poměru a jednotlivých druhů zpracování, ve které autor aplikoval obecný úvod do materie na konkrétní zpracování, k nimž v aplikační praxi na pracovišti dochází. V rámci této práce se nedostalo větší pozornosti např. v dnešním globalizovaném světě velmi aktuální problematice předávání osobních údajů, správnému trestání nejen ze strany UOOU, ale také inspektorátu práce či zpracování biometrických údajů zaměstnanců.

Co se sledování zaměstnanců týče, tak autor považuje nastolenou judikaturu za velmi rozumnou. Dle autora nelze z hlediska ochrany osobních údajů rezignovat také na zájmy zaměstnavatele a tolerovat zaměstnancům neplnění svých povinností. Na druhou stranu je potřeba nastavit určité mantinely sledování zaměstnanců, což se soudům poměrně povedlo. Jisté je to, že daných případů bude jen přibývat a bude velmi zajímavé sledovat následující judikaturu.

Co se právní úpravy ochrany osobních údajů v návaznosti na pracovněprávní vztahy týče, tak dle názoru autora je tato problematika pro zaměstnavatele a v důsledku i pro samotné zaměstnance velmi nepřehlednou, a to především z důvodu, že je potřeba aplikovat vícero právních předpisů.

Přestože autor nepovažoval přijetí Obecného nařízení za naprostou nutnost, spatřuje v něm jedno obrovské pozitivum, a to, že se této problematice bude věnovat daleko více lidí, a tím by se mohlo pozvednout obecné povědomí o této problematice. Konkrétně samotní zaměstnavatelé by pod hrozbou vysokých sankcí měli být motivováni k dodržování ochrany osobních údajů svých zaměstnanců.

Velcí zaměstnavatelé by, dle názoru autora, měli být na pozoru, protože jim přibude mnoho povinností. Z jejich strany bude nutné pečlivě provést audit zpracovávaných údajů a důkladně se na změny připravit. Je pravděpodobné, že z jejich strany bude určitá nevole, a to zejména s ohledem na to, že prováděné změny je budou stát velké náklady, ale dle názoru autora je i to znamením, že se tato problematika začne brát vážněji.

Autor dále velmi pozitivně hodnotí práci WP 29 a UOOU, kteří se po celou dobu účinnosti Směrnice, respektive Zákona, věnovali aktuálním tématům a svými stanovisky pomáhali odstranit některé aplikační nejasnosti.

Závěrem se autor domnívá, že se mu podařilo naplnit vymezené cíle této práce a v dostatečném rozsahu přiblížil danou problematiku a získané poznatky následně aplikoval na jednotlivé zpracování osobních údajů zaměstnanců.

Seznam zkratek

ESLP	Evropský soud pro lidská práva
EU	Evropská unie
GPS	Geo Positioning System
Evropská úmluva	Úmluva o ochraně lidských práv a svobod
KSČ	Komunistická strana Československa
Listina	Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky
Listina EU	Listina základních práv Evropské unie
MVČR	Ministerstvo vnitra České republiky
NSS	Nejvyšší správní soud České republiky
Nejvyšší soud	Nejvyšší soud České republiky
Obecné nařízení	Nařízení EP a Rady 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
Občanský zákoník	Zákon 89/2012 Sb., občanský zákoník
OSN	Organizace spojených národů
Sb.	Sbírka zákonů
Sb. m. s.	Sbírka mezinárodních smluv
Směrnice	Směrnici EP a Rady č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
SDEU	Soudní dvůr Evropské unie
SEU	Smlouva o Evropské unii
SFEU	Smlouva o fungování Evropské unie

Trestní zákoník	Zákon č. 40/2009 Sb., trestní zákoník
UOOU	Úřad pro ochranu osobních údajů
Úmluva 108	Úmluva č. 108 o ochraně osob se zřetelem na automatické zpracování osobních dat
Ústava	Ústavní zákon č. 1/1993 Sb., Ústava České republiky
Ústavní soud	Ústavní soud České republiky
WP 29	Pracovní skupina WP 29 (<i>Article 29 Working Party</i>)
Zákon	Zákon 101/2000. Sb., o ochraně osobních údajů
Zákoník práce	Zákon 262/2006 Sb., zákoník práce
ZSPI	Zákon 106/1999 Sb., o svobodném přístupu k informacím
ZTOPO	Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim

Seznam zdrojů

Právní předpisy České republiky

- Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky
- Ústavní zákon č. 1/1993 Sb., Ústava České republiky
- Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
- Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
- Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
- Zákon č. 155/1995 Sb., o důchodovém pojištění, ve znění pozdějších předpisů
- Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů, ve znění pozdějších předpisů
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů
- Zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů
- Zákon č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů

- Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů
- Zákon. č. 187/2006 Sb., o nemocenském pojištění, ve znění pozdějších předpisů
- Zákona č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů
- Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, ve znění pozdějších předpisů
- Zákon č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
- Zákon č. 455/1991 Sb., o živnostenském podnikání, ve znění pozdějších předpisů
- Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů

Mezinárodní smlouvy a jiné mezinárodní dokumenty

- Charta OSN
- Všeobecná deklarace lidských práv
- Mezinárodní pakt o občanských a politických právech
- Mezinárodní pakt o hospodářských, sociálních a kulturních právech
- Úmluva o ochraně lidských práv a svobod z roku 1950
- Úmluva č. 108 o ochraně osob se zřetelem na automatické zpracování osobních dat
- Rada Evropy Rezoluce 428 o masových komunikačních médiích a lidských právech

- Council of Europe *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*
- Council of Europe *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.*

Předpisy EU

- Listina základních práv Evropské unie
- Smlouva o Evropské unii
- Smlouva o fungování Evropské unie
- Směrnici Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- Nařízení Evropského parlamentu a Rady 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
- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací
- Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 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
- Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci,

odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti

Judikatura

Česká judikatura

- Nález Ústavního soudu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94
- Nález Ústavního soudu ze dne 9. 3. 2004, sp. zn. Pl. ÚS 38/02
- Nález Ústavního soudu ze dne 18. prosince 2006, sp. zn. I. ÚS 321/06
- Nález Ústavního soudu ze dne 12. 3. 2008, sp. zn. Pl. ÚS 83/06
- Nález Ústavního soudu ze dne 15. 11. 2010, sp. zn. I. ÚS 517/10
- Nález Ústavního soud ze dne 22. 3. 2011, sp. zn. Pl. 24/10
- Usnesení Ústavního soudu ze dne 1. března 2000, sp. zn. II. ÚS 517/99
- Usnesení Ústavního soudu ze dne 8. 2. 2010, sp. zn. IV. ÚS 2425/09
- Usnesení Ústavního soudu ze dne 7. 11. 2012, sp. zn. I. ÚS 3933/2012
- Rozsudek Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011
- Rozsudek Nejvyššího soudu ze dne 17. 10. 2012, sp. zn. 21 Cdo 2596/2011
- Rozsudek Nejvyššího soudu ze dne 21. 1. 2014, sp. zn. 21 Cdo 1496/2013
- Rozsudek Nejvyššího soudu ze dne 7. 8. 2014, sp. zn. 21 Cdo 747/2013
- Rozsudek Nejvyššího soudu ze dne 19. 7. 2016, sp. zn. 21 Cdo 2590/2015
- Rozsudek Nejvyššího správního soudu ze dne 12. února 2009, č.j. 9 As 34/2008

- Rozsudek Nejvyššího správního soudu ze dne 5. listopadu 2009, sp. zn. 1 Afs 60/2009 – 119
- Rozsudek Nejvyššího správního soudu ze dne 27. května 2011, sp. zn. 5 As 57/2010 – 79
- Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012
- Rozsudek Městského soudu v Praze ze dne 16. 10. 2012, sp. zn. 6 Ca 378/2008-37

Zahraniční judikatura

- Rozsudek Soudního dvora EU ze dne 10. 4. 1984 ve věci 14/83, „*Van Colson*“
- Rozsudek Soudního dvora EU ze dne 13. května 2014, ve věci C 131/12 *Google Spain SL, Google Inc. Proti Agencia Española de Protección de Datos*
- Rozsudek Soudního dvora EU ze dne 19. 10. 2016 ve věci C-582/14 *Breyer proti Německo*
- Rozsudek Evropského soudu pro lidská práva ze dne 3. dubna 2007 ve věci *Copland versus Spojené království* (stížnost č. 62617/00)
- Rozsudek Evropského soudu pro lidská práva ze dne 16. prosince 1992 ve věci *Niemietz versus Německo* (stížnost č. 13710/88)
- Rozsudek Evropského soudu pro lidská práva ze dne 25. června 1997 ve věci *Halford versus Spojené království* (stížnost č. 20605/92)
- Rozsudek Evropského soudu pro lidská práva ze dne 12. ledna 2016 ve věci *Barbulescu versus Rumunsko* (stížnost č. 61496/08)

Literatura

- ALEXY, ROBERT A *Theory of Constitutional Rights*. Oxford: Oxford University Press, 2010
- BARTÍK, VÁCLAV a JANEČKOVÁ, EVA *Poskytování osobních údajů o zaměstnancích*. *Práce a mzda* [online], 2010, č. 10
- BARTÍK, VÁCLAV, JANEČKOVÁ, EVA *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 3. vydání Praha: Linde, 2013
- BĚLINA, MIROSLAV a kol. *Pracovní Právo*. 6. Doplněné a podstatně přepracované vydání. Praha: C.H. Beck, 2014
- BĚLINA, MIROSLAV, DRÁPAL, LJUBOMÍR A KOL. *Zákoník práce. Komentář*. 2 vydání. Praha : C. H. Beck, 2015
- ČEPELKA, ČESTMÍR, ŠTURMA, PAVEL *Mezinárodní právo veřejné*. 1. vydání. Praha: C.H. Beck, 2008
- FIALOVÁ, EVA *Bezkontaktní čipy a ochrana soukromí*. Praha: Leges 2016
- HŮRKA, Petr a kol. *Zákoník práce a související ustanovení občanského zákoníku* 3. aktualizované a rozšířené vydání. Olomouc: ANAG, 2014, s.952
- JANEČKOVÁ, EVA, BARTÍK, VÁCLAV *Ochrana osobních údajů v pracovním právu (Otázky a odpovědi)*. Praha: Wolters Kluwer, 2016
- KADLECOVÁ TEREZA, *GPS ve služebních vozidlech aneb malý čip = velká komplikace?* *Praktická personalistika*, Olomouc: ANAG č. 3-4/2015
- KUČEROVÁ, ALENA a kol. *Zákon o ochraně osobních údajů. Komentář*. 1 vydání. Praha : C. H. Beck, 2012
- MAŠTALKA, JIŘÍ *Osobní údaje, právo a my*. 1 vyd. Praha: C. H. Beck, 2008

- MATES, PAVEL *Ochrana osobních údajů*. Vyd. 1. Praha: Karolinum, 2002
- MATES, Pavel. *Ochrana soukromí ve správním právu*. 2. aktualizované a podstatně přepracované vyd. Praha: Linde, 2006
- MORÁVEK, JAKUB *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013
- MORÁVEK JAKUB *Sledování zaměstnanců v kontextu novely zákoníku práce*. Právní rozhledy, C. H. Beck sv. 5/2012
- NONNEMANN, FRANTIŠEK a FOLDOVÁ, VANDA *Zveřejňování platů zaměstnanců veřejné sféry ve světle aktuálního rozsudku Nejvyššího správního soudu*. Právní rozhledy, C. H. Beck sv. 2/2015
- NONNEMANN, FRANTIŠEK *Sledování aktivity zaměstnance na internetu ve světle aktuální judikatury Evropského soudu pro lidská práva*. In: Epravo.cz [online]
- NONNEMANN, FRANTIŠEK *Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů*. Právní rozhledy, C. H. Beck sv. 13-14/2012
- NONNEMANN, FRANTIŠEK *Trestní odpovědnost právnické osoby za neoprávněné nakládání s osobními údaji*. Právní rozhledy, C. H. Beck sv. 20/2016
- NONNEMANN, FRANTIŠEK a SKÁCELOVÁ, MICHAELA *Zpracování biometrických údajů ve světle obecného nařízení o ochraně osobních údajů (GDPR)* In: Epravo.cz [online]
- NOVÁK, DANIEL *Zákon o ochraně osobních údajů a předpisy související. Komentář*. Praha: Wolters Kluwer, 2014
- POTOČNÝ, MIROSLAV, ONDŘEJ, JAN *Mezinárodní právo veřejné – Zvláštní část*. 6 doplněné a rozšířené vydání. Praha: C.H. Beck, 2011

- ŠUBRT, BOŘIVOJ, TUČEK, MILAN *Pracovnílékařské služby: Povinnosti zaměstnavatelů a lékařů*. 2. doplněné vydání Olomouc: ANAG, 2015
- TOMÁŠEK, MICHAL, TÝČ, VLADIMÍR a kol. *Právo Evropské unie*. 1. Vydání. Praha: Leges, 2013
- VIDRNA, JAN, KOUDELKA ZDENĚK *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců*. 1 vydání. Praha : C. H. Beck, 2013
- WAGNEROVÁ A KOL. *Listina základních práv a svobod – Komentář*. Praha: Wolters Kluwer, 2012
- WARREN, SAMUEL; BRANDEIS, LOUIS, The Right to Privacy. in Harvard Law Review 890 Vol. IV

Stanoviska UOOU a WP 29

- Stanovisko UOOU č. 2/2001 *Zpracování citlivého osobního údaje členských příspěvků v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací*
- Stanovisko UOOU č. 1/2006 *Provozování kamerového systému z hlediska zákona o ochraně osobních údajů*
- Stanovisko UOOU č. 2/2008 *Souhlas se zpracováním osobních údajů*
- Stanovisko UOOU č. 2/2009 *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*
- Stanovisko UOOU č. 6/2009 *Ochrana soukromí při zpracování osobních údajů*
- Stanovisko UOOU č. 3/2011 *Ochrana osobních údajů podnikajících fyzických osob*

- Stanovisko UOOU č. 2/2012 *Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů*
- Stanovisko UOOU č. 4/2012 *Zpracování osobních údajů zemřelých osob*
- Stanovisko UOOU č. 6/2012 *Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů*
- UOOU *Ke zpracování osobních údajů bývalých zaměstnanců*
- WP 29 Opinion 8/2001 *on the processing of personal data in employment context*
- WP 29 Opinion 4/2004 *on the processing of personal data by means of video surveillance*
- WP 29 Opinion 4/2007 *on the concept of personal data*
- WP 29 Opinion 1/2010 *on the concepts of the „controller“ and „processor“*
- WP 29 Opinion 3/2012 *on developments in biometric technologies*

Další prameny

- BAJÁKOVÁ, EVA *Newsletter: Revoluce v právu ochrany osobních údajů bude v roce 2018*
- Česká televize *Fotka na Facebooku může uchazeči o práci podrazit nohy.*
- Důvodová zpráva k zákonu č. 101/2000 Sb., o ochraně osobních údajů
- Evropská Unie *Shrnutí legislativy EU*
- Forbes *Mark Zuckerberg: 2 Billion Users Means Facebook's 'Responsibility Is Expanding'*

- International Labour Organization *Code of practice on the protection of workers' personal data*
- KUNEVA, MEGLENA *Keynote Speech. Roundtable on Online Data Collection, Targeting and Profiling*
- Rozhodnutí UOOU ze dne 10. 3. 2004, č.j. 1233/03-3000/892/03-OLP
- Rozhodnutí UOOU ze dne 3. 7. 2013, č.j. UOOU-00237/13-38
- *Sněmovní tisk č. 911/0 - Vládní návrh zákona, kterým se mění zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a další související zákony*
- Sdělení Ministerstva zahraničních věcí č. 29/2005 Sb. m. s. o sjednání *Dodatkového protokolu k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice*
- UOOU a MVČR *Metodické doporučení k poskytování informací o platech pracovníků povinných subjektů podle zákona o svobodném přístupu k informacím*
- UOOU *Ochrana osobních údajů na pracovišti*
- UOOU *Provozování kamerových systémů: Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů*
- VEŘEJNÝ OCHRÁNCE PRÁV *Souhrnná zpráva o činnosti veřejného ochránce práv 2013*

Resumé

Tato práce se zabývá ochranou osobních údajů v návaznosti na pracovněprávní vztahy. Vzhledem k tomu, že problematika ochrany osobních údajů je velmi rozsáhlá, není cílem této práce podat všezahrnující výklad, nýbrž přiblížení obecné právní úpravy s objasněním základních pojmů a jejich následnou aplikací na pracovněprávní vztahy.

Autor rozděluje tuto práci do 6 kapitol a kromě relevantní právní úpravy věnuje svoji pozornost také nejdůležitější judikatuře a stanoviskům jak WP 29, tak UOOU, které vykládají některé aplikační nejasnosti.

S ohledem na to, že ochrana osobních údajů je integrálně spjata s nedotknutelností člověka a soukromím, je první část této práce věnována právě pojmu soukromí a jeho vymezení.

V druhé kapitole je rozebrána právní úprava ochrany soukromí a osobních údajů. Tato kapitola zahrnuje jak mezinárodní, regionální, tak také českou právní úpravu, která vychází zejména ze směrnice Evropského parlamentu a Rady č. 95/46/ES.

Ve třetí kapitole se autor věnuje základnímu pojmosloví ochrany osobních údajů, jehož vymezení je důležité nejen pro chopení daného téma, ale i pro samotnou aplikaci na dané případy.

Čtvrtá kapitola je zaměřena na povinnosti zaměstnavatele jako správce osobních údajů a práva zaměstnance jako subjektu údajů. V této kapitole autor také vypichuje některé změny, které přináší Obecné nařízení Evropského parlamentu a Rady 2016/679, které nabyde účinnosti v květnu 2018.

Pátá kapitola popisuje zpracování osobních údajů před vznikem, v průběhu a po skončení pracovního poměru.

A konečně šestá kapitola je zaměřena na sledování zaměstnanců, které je v současnosti velice aktuálním tématem. Autor v této kapitole dále popisuje jednotlivé případy monitoringu zaměstnanců, a to sledování aktivity zaměstnanců na internetu, monitorování e-mailové korespondence a služebních telefonů zaměstnanců, kontrole služebních automobilů a kamerovým systémům na pracovišti.

Summary

This thesis deals with the protection of personal data in relation to the labour law relationships. Considering the extensiveness of the topic of personal data protection, the aim of this thesis is not giving an all-encompassing explanation, however, to introduce the general legal regulations together with the explanation of the principal legal concepts and their subsequent application on the labour law relationships.

The author divides this thesis into 6 chapters. Apart from the relevant legal regulations the author focuses on the main case law and opinions issued by WP 29 and UOOU (the Office for Personal Data Protection) as well, which interpret some legal uncertainties.

By reason that the personal data protection is integrally connected to the inviolability of the person and privacy itself, the first chapter focuses on the concept of privacy and its interpretation.

The second chapter discusses the privacy and data protection legal regulation. This chapter covers both international, regional and also Czech legislation, which particularly emanates from the European Parliament and Council Directive 95/46/EC.

In the third chapter, the author focuses on the basic concepts of the personal data protection. Its explanation is necessary not only for understanding of this topic, but also for the subsequent application to the specific cases.

The fourth chapter devotes to the employer's duties as a data controller and the rights of the employees as a data subjects. In this chapter, the author also outlines some changes which the General Regulation 2016/679 of the European Parliament and Council, introduces. The General Regulation will be effective as of the May 2018.

The fifth chapter describes the processing of the personal data before the beginning, in the course of and after termination of the employment contract.

Finally, the sixth chapter is focused on the monitoring of employees, which currently represents up to date topic. In this chapter, the author also describes particular types of employee monitoring, namely the screening of internet use, checking of e-mail correspondence and telephones of employees, control of company cars and/or camera surveillance systems at workplace.

Klíčová slova

- Osobní údaj
- Pracovněprávní vztahy
- Sledování zaměstnanců

Keywords

- Personal data
- Labour law relationships
- Monitoring of employees

Název práce v anglickém jazyce

Personal Data Protection and Labour Law Relationships