UNIVERZITA KARLOVA

Právnická fakulta

Mgr. Ing. Jaroslav Zahradníček

Ochrana osobnosti a osobních údajů v pracovněprávních vztazích

Disertační práce

Školitel: doc. JUDr. Petr Hůrka, Ph.D.

Studijní program: Teoretické právní vědy

Datum vypracování práce (uzavření rukopisu): 6. června 2019

Prohlašuji, že jsem předkládanou disertační práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 564 134 znaků včetně mezer.

……..
Mgr. Ing. Jaroslav Zahradníček

V Praze dne 6. června 2019

Poděkování

Za pragmatické vedení v průběhu celého studia patří mé díky školiteli doc. Hůrkovi. Dále bych chtěl poděkovat zejména mým kolegům Mgr. Drahomíru Tomašukovi a Mgr. Martinovi Kubíkovi, kteří mě k ochraně soukromí a osobních údajů přivedli a *de facto* mi umožnili se této problematice v praxi věnovat již téměř deset let. V neposlední řadě děkuji též mé snoubence a mé rodině za trpělivost při psaní této práce a podpoře při jejím vyhotovení.

Obsah

Úvod ... 11
I. ČÁST PRÁVNÍ RÁMEC A VÝCHODISKA ... 18
1 Právní rámec ... 18
1.1 Prameny národní ... 18
1.1.1 Základní předpisy ... 18
1.1.2 Další zákonné normy ... 20
1.1.3 Ústavní předpisy a ostatní právní normy ... 20
1.2 Předpisy Evropské unie ... 21
1.2.1 Sekundární právo Evropské unie ... 21
1.2.2 Primární právo EU ... 22
1.2.3 Ostatní prameny ... 24
1.3 Mezinárodní prameny ... 25
1.3.1 Rada Evropy ... 25
1.3.2 Ostatní prameny ... 27
2 Východiska ochrany osobnosti a osobních údajů ... 30
2.1 Právo na ochranu osobnosti ... 30
2.1.1 Ochrana osobnosti jako základní lidské právo ... 31
2.1.2 Ochrana osobnosti dle platné právní úpravy ... 32
2.1.3 Možnosti ochrany osobnostních práv ... 34
2.1.4 Složky práva na ochranu osobnosti ... 36
2.1.5 Limitace práva na ochranu osobnosti ... 37
2.2 Ochrana soukromí ... 39
2.2.1 Pojem a podsložky ochrany soukromí ... 40
2.2.2 Vývoj ochrany soukromí ... 41
2.2.3 Ochrana soukromí v rozhodnutích soudů ... 43
2.3 Úvodní poznámky k ochraně osobních údajů ... 46
2.3.1 Historie ochrany osobních údajů ... 46
2.3.2 Ochrana před neoprávněným zpracováním osobních údajů ... 47
2.4 Vztah ochrany osobnosti a osobních údajů ... 48
2.4.1 Podobné, nikoliv však stejné množiny ... 49
2.4.2 Další odlišnosti ... 51
2.4.3 Shrnutí ... 52
II. ČÁST OCHRANA OSOBNOSTI ... 54
3 Úvodní východiska ochrany osobnosti v pracovním právu ... 54
3.1 Vztah zaměstnance a zaměstnavatele ... 54
3.2 Charakter právních norem pracovního práva ... 57
3.3 Legitimní očekávání soukromí ... 58
3.4 Ochrana, i když není rozumné očekávat soukromí ... 61
4 Ochrana osobnosti zaměstnanců v čase ... 65
4.1 Ochrana před vznikem pracovního poměru ... 65
4.1.1 Pohled do zahraničí ... 66
4.1.2 Situace v ČR ... 69
4.1.3 Zákon o zaměstnanosti ... 71
4.1.4 Antidiskriminační zákon ... 72
4.1.5 Shrnutí ... 74
4.2 Ochrana po skončení pracovního poměru ... 75
4.2.1 Pracovní posudek ... 75
4.2.2 Černé seznamy (blacklisty) ... 77
4.3 Ochrana osobnosti zaměstnance mimo výkon práce ... 80
4.3.1 Soukromý život zaměstnance ... 81
4.3.2 Osobní spis zaměstnance ... 85
5 Ochrana osobnosti zaměstnance při výkonu práce ... 88

5.1 Kontrola vnášených věcí 89
5.1.1 Zákaz vnášení předmětů 91
5.2 Obecné poznámky k ustanovení § 316 ZPr 93
5.3 Kontrola svěřených prostředků 94
5.3.1 Zákaz využívání 96
5.3.2 Dovolené využívání 98
5.3.3 Přiměřený způsob kontroly 99
5.4 Kontrola, existuje-li závažný důvod 103
5.4.1 Vzájemný vztah kontrolních oprávnění 103
5.4.2 Podmínky pro aplikaci kontrolního oprávnění 105
5.4.3 Obsah kontrolního oprávnění 108
5.4.4 Informační povinnost zaměstnavatele 109
5.4.5 Aplikace ustanovení v praxi 111
5.4.6 Shrnutí 112
5.5 Chráněné zájmy zaměstnavatele 113
5.5.1 Odpovědnost zaměstnavatele za jednání zaměstnance 114
III. ČÁST OCHRANA OSOBNÍCH ÚDAJŮ ZAMĚSTNANCŮ 118
6 Východiska a právní základy zpracování osobních údajů 118
6.1 Vymezení působnosti a pojmů 118
6.1.1 Působnost 119
6.1.2 Pojmy 120
6.2 Zákonnost zpracování a účelové omezení 125
6.2.1 Plnění právních povinností 128
6.2.2 Plnění smluvního vztahu 132
6.2.3 Oprávněný zájem 134
6.2.4 Souhlas 139
6.2.5 Více právních základů 144
7 Zásady a vybrané aspekty zpracování údajů zaměstnanců 147
7.1 Transparentnost 147
7.2 Práva zaměstnanců 149
7.2.1 Právo na přístup k osobním údajům 150
7.2.2 Právo na výmaz 152
7.2.3 Právo vznést námitku 154
7.2.4 Ostatní práva 155
7.3 Minimalizace údajů 157
7.3.1 Jednotlivé údaje zpracovávané zaměstnavateli 159
7.4 Zvláštní kategorie osobních údajů 163
7.4.1 Informace o zdravotním stavu 165
7.4.2 Členství v odborové organizaci 166
7.4.3 Odsouzení za trestný čin 167
7.4.4 Biometrické údaje 168
7.4.5 Shrnutí 170
7.5 Omezení uložení 171
7.5.1 Doba zpracování osobních údajů zaměstnanců 173
7.6 Zpřístupňování údajů třetím osobám 176
7.6.1 Předávání jiným správcům 176
7.6.2 Předávání zpracovatelům 179
7.6.3 Vybrané další případy předávání 181
7.7 Záznamy o činnostech, integrita a důvěrnost osobních údajů 183
7.7.1 Záznamy o činnostech zpracování 183
7.7.2 Zabezpečení osobních údajů 185
7.7.3 Posouzení vlivu na ochranu osobních údajů 187
7.7.4 Pověřenec pro ochranu osobních údajů 189
IV. ČÁST VYBRANÉ APLIKAČNÍ OTÁZKY A SHRNUTÍ 191
8 Vybrané praktické aspekty ochrany zaměstnanců 191

8.1 Monitoring zaměstnanců v praxi ... 191
8.1.1 Písemnosti zaměstnanců (kontrola listovních zásilek) ... 191
8.1.2 Elektronická komunikace – e-maily ... 193
8.1.3 Využití informačních technologií, prohlížení webu ... 196
8.1.4 GPS ... 200
8.1.5 Kamery ... 202
8.2 Whistleblowing ... 206
8.3 Odhalování majetku zaměstnanců ... 208
9 Komparativní pohled a zamyšlení de lege ferenda ... 210
9.1 Komparativní pohled ... 210
9.2 De lege ferenda ... 214
Závěr ... 218
Seznam zkratek ... 224
Seznam použitých zdrojů ... 225
Seznam použité literatury ... 225
Seznam časopiseckých článků ... 226
Seznam použitých internetových zdrojů ... 228
Seznam použitých právních předpisů ... 232
Seznam použité judikatury ... 234
Seznam ostatních zdrojů ... 237
Abstrakt ... 239
Abstract ... 240

Úvod

Doslova bestsellerem v branži poskytování právních, poradenských či informačních služeb se v letech 2017 a 2018 stala nová regulace ochrany osobních údajů, dobře známá pod zkratkou „GDPR“. GDPR je nařízení Evropské rady a parlamentu č. 2016/679, obecné nařízení o ochraně osobních údajů (dále jen jako „nařízení GDPR“). Bez ohledu na skutečnost, že popularitu této regulaci zařídily bezpochyby značné sankce, které hrozí za porušení stanovených pravidel (o tom svědčí skutečnost, že právní úprava, kterou nařízení GDPR nahradilo, nestanovila diametrálně odlišná pravidla od těch, která jsou „nově“ vyžadována podle nařízení GDPR), došlo díky této právní úpravě k relevantnímu vyzdvihnutí této problematiky a obecně též problematiky ochrany osobnosti a soukromí mezi „o trochu širší“, nikoliv však ještě „širokou“ veřejnost. To je zásluha, kterou si předchozí právní úprava vycházející ze směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „Směrnice“), nedokázala připsat.

Že v dnešní době dostává ochrana soukromí a osobních údajů citelně zabrat, je všem snad už zřejmé. Naše společnost je více než kdy jindy digitalizovaná a globalizovaný svět umožňující okamžité sdílení jakýchkoliv informací bez ohledu na vzdálenosti a zeměpisné hranice a zároveň snadné analytické zpracovávání těchto informací definitivně přepsaly chápání pojmu soukromí a způsoby jeho ochrany. Ve světle známé skutečnosti, že technologický vývoj obvykle předchází přijetí odpovídající právní úpravy regulující danou otázku, je nutné se této problematice důkladně věnovat a pružně reagovat na další pokrok, který ještě bezpochyby není zastaven. Zejména tempo rozvoje schopnosti automatizovaného zpracování velkého množství informací[1] ovlivňuje všechny jednotlivce a jejich osobnost či soukromí v jejich každodenním životě.

O to více pak platí, že ochrana osobnosti a soukromí je důležitější ve vztahu dvou či více osob, kdy některé z nich jsou ve slabším postavení než ostatní. To platí zejména pro vztah zaměstnance a zaměstnavatele, který je předmětem této práce. Zasahování do osobnostní sféry zaměstnanců se pro zaměstnavatele stalo snazším než kdy předtím. Široké využití informačních technologií a související automatizace procesů na pracovišti umožňují

[1] V anglickém jazyce označováno též jako „Big Data“.

například snadné monitorování výkonu zaměstnance, sledování toho, kdy čerpá pauzy a jak je tráví, jak spolupracuje s ostatními zaměstnanci nebo jak využívá svěřené prostředky. Spolu s všudypřítomnými kamerami, rozšířením používání technologických zařízení, ale i v souvislosti s rozmachem sociálních sítí je pak postavení dnešních zaměstnanců o to citlivější.

Je to právě zmíněný rozvoj sociálních sítí a komunikačních technologií, který má za následek další důležitý fakt, a to že osobní sféra zaměstnance se v mnohem větší míře prolíná se sférou pracovní. Dnes to nejsou již jen vyšší manažeři, kteří mají pracovní notebooky, mobily, tablety či jiná podobná zařízení. Právě naopak, dnes už každý druhý dopravce či pošťák dostane služební telefon se SIM-kartou, ze kterého kontaktuje zákazníky svého zaměstnavatele, mnoho techniků či operátorů má technické nástroje, které vedou detailní informace o jejich pracovní činnosti, osobní počítač je dnes rozšířen prakticky na veškeré „kancelářské“ pozice, nezřídka je těmto zaměstnancům dokonce svěřen notebook, který nevyužívají jen na pracovišti, ale i na služebních cestách, případně při tzv. *home office*.

K výše uvedenému dochází mimo jiné díky rozšíření flexibilních forem práce, kdy zaměstnanci využívají svěřené pracovní prostředky i doma nebo na cestách, což má nevyhnutelně za následek, že tyto prostředky jsou využívány i pro soukromé potřeby, ať už je to s vědomím zaměstnavatele, či bez něj. Toto přitom neplatí jen o hardwaru, který mají zaměstnanci od zaměstnavatele, ale rovněž pro telefonní čísla, e-mailové adresy, účty na sociálních sítích apod. Když tedy následně může být jeden notebook s pracovní e-mailovou schránkou někdy využíván pro pracovní účely a jindy pro soukromé, je zřejmé, že není možné vytyčit ostrou hranici mezi těmito dvěma světy. Mnohdy dokonce může mít jeden e-mail zčásti pracovní a zčásti soukromý charakter.

Zaměstnanci mnohdy tyto informace zaměstnavatelům nabízejí na „zlatém podnosu“, zejména pokud využívají pracovní prostředky pro soukromé účely, ačkoliv to mají od zaměstnavatele zakázáno. Na první pohled poněkud „obtížnější“ může být situace pro zaměstnavatele, pokud svým zaměstnancům dovolí užívat svěřené prostředky pro soukromé potřeby, v obou případech je však zřejmé, že ochrana osobnosti zaměstnance a jeho soukromí bude stejná. Zaměstnavatelé mohou ale do soukromí zasahovat i jinými prostředky a jinými cestami. Kdekterý zaměstnanec může mít otevřený profil na svých sociálních sítích a vyjadřovat se tam nelichotivě o svém zaměstnavateli.

Nabízelo by se pak jednoduché řešení ze strany zaměstnance, jak výše uvedeným skutečnostem předcházet, kterým by bylo omezení přístupu na profil zaměstnance,

a i v jiných ohledech obezřetnější jednání zaměstnanců. To je pravda jen částečně, neboť ani velká obezřetnost nemusí být dostačující. V uzavřeném profilu mohou zaměstnance „udat" jeho závistiví kolegové. Případně platí, že zaměstnanec bude stěží znát, jaké veškeré (skryté) sledovací prostředky zaměstnavatel používá. Dokonce často není pro zaměstnavatelovo rozhodnutí o rozvázání pracovního poměru nutné jakékoliv přímé vyjadřování. Mnohdy stačí dát „*like*" vyjádření jiného, stačí „sledovat" extrémistickou politickou stranu, stačí zúčastnit se nějaké demonstrace. Skutečnost, že zaměstnavatelé toto mnohdy sledují, není schizofrenní představou o dnešním světě ale smutnou realitou dnešní doby.[2] Nemá pak takovéto jednání zaměstnavatele diskriminační charakter a nezasahuje zaměstnavatel takovým jednáním nadmíru do soukromého života zaměstnanců?

Dokonce ani dříve, než došlo k tak mohutnému rozšíření informačních technologií a k digitalizaci běžného života, tomu nebylo jinak. Přestože tyto možnosti monitorování zaměstnanců nebyly dříve tak snadné, zaměstnavatelé neváhali sáhnout po jiných dostupných nástrojích a za tyto vynaložit finanční prostředky. Příkladem může být skandál z Francie, kdy tamní vedení společnosti IKEA spolu s dalšími osobami, včetně policistů, údajně nedovoleně sledovali své zaměstnance, zejména ty, kteří byli členy odborových organizací. Sledovali dokonce také zákazníky, kteří měli se společností spory (vedli se společností reklamace či si na ni stěžovali), a vyhledávali o nich soustavně informace, které by mohli použít proti nim. Za tyto činnosti přitom vynakládali nemalé finanční prostředky. Obdobné informace byly získávány též ohledně uchazečů o zaměstnání. Nešlo přitom o nějaký nahodilý případ, nýbrž o soustavné vyhledávání informací za pomoci soukromých detektivů, či dokonce příslušníků policie.[3] Případ byl odhalen až v návaznosti na to, kdy společnost IKEA ukončila pracovní poměr se svou lokální manažerkou (mající pracovní poměr trvající přes 12 let u společnosti) poté, co za pomoci soukromého detektiva, kterému mimochodem o své zaměstnankyni předala veškeré jí dostupné soukromé informace, zjistila, že zaměstnankyně lhala o důvodu své nepřítomnosti v práci, když nebyla nemocná, jak

[2] Z výsledků studie provedené v roce 2012 v USA ve státě Connecticut vyplynulo, že 90 % náborářů si prověřuje uchazeče o zaměstnání na internetu (Can Social Media Get You Fired, Elizabeth Garone in BBC Capital, 3. listopadu 2014 [online]. [cit. 2018-11-05]. Dostupné z: http://www.bbc.com/capital/story/20130626-can-social-media-get-you-fired)

[3] French prosecutors push for Ikea trial over spying charges. In The Local.se, 11. ledna 2018 [online]. [cit. 2018-11-05]. Dostupné z: https://www.thelocal.se/20180111/french-prosecutors-push-for-ikea-trial-over-spying-charges

tvrdila. Daná zaměstnankyně se tímto cítila natolik ponížena a zrazena, že se následně pokusila o sebevraždu.[4]

Ač je výše uvedený příběh v jistých ohledech extrémní, je nepochybné, že informace o soukromí zaměstnanců jsou pro zaměstnavatele cennými informacemi a zaměstnavatelé mají mnoho důvodů, proč je shromažďovat. Tím základním je obvykle ochrana jejich majetku a další rozvoj jejich podnikání. Ale může se jednat i o jiné pohnutky zaměstnavatele, které nebudou v souladu se zákonem, například šikanózní chování a osobní neshody s některými zaměstnanci. Proti tomu stojí protichůdný zájem zaměstnanců na tom, aby nebylo do jejich osobních životů nijak zasahováno a aby o nich nebyly vyhledávány a shromažďovány žádné informace. Hranice těchto světů jsou neostré. Zákon se je určitým způsobem snaží vymezit, ale objektivně vzato musí mnohdy zůstávat obecným, aby v rámci své obecnosti postihoval všechny situace, které mohou nastat. Předmětem této práce je pak především zkoumáním těchto hranic v různých fázích vztahu zaměstnance a zaměstnavatele.

V rámci úvodu je nutné vymezit chápání a používání pojmů v této práci. Důležité je především chápání pojmů ochrana osobnosti a ochrana soukromí. Pojem ochrany osobnosti je v této práci vztažen k ochraně osobních údajů, a zaměřuje se proto na tuto část ochrany osobnosti, která souvisí s ochranou soukromí zaměstnance,[5] a to bez ohledu na to, že pod ochranu osobnosti zaměstnanců lze zahrnout též celou řadu dalších aspektů (například život, zdraví, čest apod.).[6] Výklad o těchto dalších aspektech však není předmětem této práce. Vedle toho také platí, že ačkoliv se v této práci obvykle píše jen o pracovním poměru, lze závěry vztáhnout obdobně též na práce konané mimo pracovní poměr,[7] kterými jsou dohoda o provedení práce a dohoda o pracovní činnosti.

Pokud jde o obsah této práce, je rozdělena na čtyři hlavní části. První část je spíše popisná a představuje jakýsi úvod do problematiky. První kapitola se věnuje relevantním právním pramenům (na vnitrostátní i mezinárodní úrovni), a to pramenům nejrůznější právní síly, včetně relevantních nezávazných (soft law) pravidel. Druhá kapitola následně popisuje východiska pro správné chápání problematiky ochrany osobnosti a osobních údajů.

---

[4] Revelations That Ikea Spied on Its Employees Stir Outrage in France. In The New York Times, 15. prosince 2013 [online]. [cit. 2018-11-05]. Dostupné z: https://www.nytimes.com/2013/12/16/business/international/ikea-employee-spying-case-casts-spotlight-on-privacy-issues-in-france.html

[5] Obdobně ochranu osobních práv či ochranu osobnosti zaměstnance chápe též učebnice pracovního práva (Bělina, M. a kol. *Pracovní právo.* 7. doplněné a podstatně přepracované vydání 2017. Praha: C. H. Beck, 2017, s. 166).

[6] Srov. blíže výklad v bodě 2.1.4.

[7] Srov. ustanovení § 77 odst. 2 ZPr.

Druhá a třetí část se postupně věnují vždy samostatně ochraně osobnosti a ochraně osobních údajů (s určitými překryvy). Důvodem pro takové rozdělení práce je autorovo vnímání těchto dvou oblastí a reflexe současné právní úpravy, která, jak bude vysvětleno, neposkytuje výslovné propojení mezi těmito dvěma fenomény a nutí tak právní teorii, aby tento nedostatek odstraňovala. V rámci druhé části je analýza zaměřena nejen na zkoumání platných ustanovení obsažených v zákoně č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „ZPr"), ale i na různé životní situace, při kterých může docházet k zásahům do ochrany osobnosti zaměstnanců. Zvlášť jsou analýze podrobena specifika vztahů mezi zaměstnavatelem a zaměstnancem, možnost zaměstnavatele vyžadovat od zaměstnanců určité specifické informace, různé fáze vztahu mezi nimi, a především kontrolní oprávnění zaměstnavatelů a jejich konflikty s osobnostními právy zaměstnanců.

Třetí část se plně věnuje ochraně osobních údajů zaměstnanců, a to především detailní analýze nové právní úpravy obsažené v rámci nařízení GDPR. V rámci toho jsou předmětem rozboru s ohledem na specifika vztahu zaměstnance a zaměstnavatele postupně jednotlivé aspekty, jako je terminologie, právní základy zpracování, informační povinnosti, práva zaměstnanců a jiné povinnosti zaměstnavatelů vyplývající ze skutečnosti, že zpracovávají osobní údaje svých zaměstnanců. I v této části jsou předmětem zkoumání různé fáze vztahu mezi zaměstnancem a zaměstnavatelem. Pozornost je věnována též možnému předávání osobních údajů zaměstnanců třetím stranám.

Čtvrtá část se věnuje vybraným praktickým otázkám a zejména rozboru konkrétních sledovacích opatření, která zaměstnavatelé v praxi nejčastěji využívají. Při tomto rozboru je blíže uvažována nutnost aplikace právních norem ochrany osobnosti i osobních údajů. Rovněž je v této závěrečné části nabídnut pohled na vybrané zahraniční právní normy a v souvislosti s tím jsou shrnuty i některé úvahy de lege ferenda.

Pokud jde o cíle této práce, je z názvu práce patrné, že primárním cílem je analýza ochrany osobnosti a osobních údajů v pracovněprávních vztazích. Tento primární cíl lze přitom dále blíže rozvést v souladu s dělením této práce na jednotlivé části a kapitoly. Dalo by se tak říci, že každá jednotlivá kapitola má svůj určitý cíl a také že cíle jednotlivých kapitol z hlediska svého významu a složitosti postupně gradují. První dvě kapitoly jsou proto spíše deskriptivní. Jejich cílem je zmapovat rozsah zkoumané právní problematiky, a to

poskytnutím přehledu relevantních právních pramenů[8] a dále též zkoumáním obecných teoretických východisek ochrany osobnosti (bez toho, aniž by byla zkoumána specifika pracovněprávních vztahů). Významnějším cílem druhé kapitoly je pak rozbor vztahu mezi ochranou osobnosti (či soukromí) a ochranou osobních údajů. S ohledem na relativní „mladost" problematiky ochrany osobních údajů nabízí tento vztah mnoho otázek, na které se autor této práce snaží nalézt odpověď.

Dalším cílem je analýza konceptu ochrany osobnosti ve smyslu ochrany soukromí. Nejprve v obecné rovině a následně ve vztahu mezi zaměstnancem a zaměstnavatelem, a to zejména s ohledem na existující faktickou nerovnost vztahu mezi nimi. Záměrem je prozkoumat možnosti limitace ochrany těchto práv a dát je do kontrastu s právy, která takovou limitaci umožňují. To vše ve smyslu příslušné právní úpravy na ústavní a zákonné úrovni. Zohledněna je též samozřejmě relevantní judikatura a právní teorie. V případě zjištěných nedostatků je vždy rovněž cílem podat vlastní návrh na odstranění takových nedostatků.

Jak je z názvu práce patrné, cílem je též analýza ochrany osobních údajů, spočívající zejména v bližší analýze jednotlivých ustanovení nařízení GDPR jakožto nového právního předpisu.[9] V tomto případě nicméně není s ohledem na rozsah problematiky záměrem analyzovat tuto problematiku obecně, nýbrž je analýza vztažena rovnou na specifické otázky vztahu mezi zaměstnancem a zaměstnavatelem. Konečně je cílem také analyzovat vybrané specifické problémy při kontrolách prováděných zaměstnavatelem, a to z hlediska nejčastěji v praxi se vyskytujících kontrolních mechanismů. Snahou je jasně definovat podmínky takových kontrolních mechanismů a nalézt meze či limity jejich využití. Zde je brána v potaz nejen relevantní právní úprava ochrany osobnosti a ochrany osobních údajů, ale opět též judikatura a případné právně nezávazné dokumenty. V návaznosti na zjištěné nedostatky je rovněž cílem nabídnout autorův pohled na možné legislativní vyřešení některých sporných otázek.

Pokud jde o metody zvolené v rámci této práce, je volena především analytická a deskriptivní metoda zkoumání předmětné problematiky, která je založena na analýze a popisu právní úpravy, relevantní judikatury, ať už české, či příslušných evropských soudů,

[8] Provedené je nezbytné pro následný výklad, jelikož jen znalost veškerých příslušných právních pramenů umožní detailní právní analýzu a nalezení správných odpovědí na zkoumané problémy.
[9] Byť zásadních novinek není mnoho (ačkoliv byla široká veřejnost často přesvědčena či přesvědčována o opaku).

a také na kritické analýze a hodnocení příslušné české právní teorie. Pokud jde o ochranu osobních údajů, je bližší pozornost věnována rovněž právně nezávazným dokumentům vydávaným na české i evropské úrovni. Jde tedy zejména o stanoviska Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“) anebo stanoviska Pracovní skupiny zřízené podle článku 29 Směrnice (dále jen „WP29“). V té souvislosti jsou pak dle potřeby různě využívány jednotlivé metody interpretace. Do určité míry je využita též komparativní metoda, například historická komparativní metoda při analýze ochrany osobních údajů nebo komparace s jinými právními řády při výkladu o konceptu ochrany soukromí či při hledání různých přístupů k řešení určitých problémů. Tato metoda nicméně není pro účely této práce klíčová a slouží spíše k zamyšlení nad možnou podobou právní úpravy *de lege ferenda*.

Prostřednictvím výše popsaných metod se autor této práce snaží nalézt odpovědi na vytyčené otázky, a to včetně nalezení obecné odpovědi, do jaké míry plní příslušné právní normy ochrannou funkci a zda je taková ochrana skutečně efektivní. Spolu s tím rovněž autor využívá svých praktických znalostí z téměř každodenního řešení otázek souvisejících s ochranou osobnosti a osobních údajů zaměstnanců a z působení ve funkci pověřence pro ochranu osobních údajů v rámci koncernu několika společností, které zaměstnávají celkem asi tisíc zaměstnanců.

I. ČÁST PRÁVNÍ RÁMEC A VÝCHODISKA

1 Právní rámec

Přestože je záměrem této práce věnovat se spíše praktickým otázkám každodenního života, nelze žádnou právní otázku důkladně zanalyzovat, aniž by se určitá část právního rozboru věnovala otázce pramenů práva a aniž by bylo na úvod zřejmé, z čeho bude takový rozbor vycházet. Výjimkou není ani tato práce. Důraz je kladen zejména na prameny formální, tj. vnější formu právních norem.[10]

Prameny je obvyklé řadit dle právní síly, a to od nejvyšší právní síly k nejnižší. V této práci je nicméně řazení pramenů práva netradiční a odpovídá praktické důležitosti pramenů pro zvolené téma a jejich praktickému využívání v situacích, kdy dochází k aplikaci konkrétních norem. Důvodem je snaha autora o vyzdvihnutí relevantních norem již na samotný úvod. Přitom však z důvodu systematičnosti zůstává zachováno členění na právní prameny národní (či vnitrostátní), evropské (přijaté na půdě EU) a mezinárodní.

Pokud jde o obsah podaného výkladu, ty prameny, které jsou pro tuto disertační práci klíčové, jsou v této kapitole pouze stručně zmíněny, jelikož se na ně následně zaměřuje další text práce. Naopak větší pozornost je věnována ostatním právním pramenům, které jsou pro ochranu osobnosti a osobních údajů zaměstnanců rovněž důležité, avšak z různých důvodů není relevantní se jimi blíže zabývat (zejména proto, že jsou příliš specifické, obsahově se shodují s jinými prameny nebo během času ztratily na významu).

1.1 Prameny národní

Národních pramenů pro zkoumanou problematiku je nepřeberné množství. Je však relativně jednoduché určit alespoň ty právní normy, které jsou adresátům nejblíže a které obsahují pro téma této práce to nejdůležitější.

1.1.1 Základní předpisy

Základní právním předpisem upravujícím pracovněprávní vztahy je ZPr. Ač je primárním smyslem tohoto právního předpisu v podstatě komplexní řešení vztahů mezi zaměstnancem a zaměstnavatelem a otázkám ochrany soukromí se věnuje jen v několika

[10] Gerloch, A. in Hendrych, D. a kol. *Právnický slovník*. 3. podstatně rozšířené vydání. Praha: C. H. Beck, 2009, pojem Pramen práva.

vybraných pasážích, jde o klíčový právní předpis pro předmět této práce. Důvodem je skutečnost, že v podstatě jen tyto normy obsažené v ZPr a s nimi bezprostředně související předpisy odlišují obecnou ochranu osobnosti a osobních údajů od té, která se týká zaměstnanců a ke které dochází v pracovněprávních vztazích.

ZPr se této problematice věnuje v několika ustanoveních, z nichž podle názoru autora této práce je nejvýznamnější zejména ustanovení § 316 ZPr, které se týká mimo jiné možnosti kontroly a sledování zaměstnanců či možnosti vyžadování specifických osobních údajů a které bude zevrubně rozebráno dále v této práci. Za zmínku dále stojí ustanovení § 30 odst. 2 týkající se možnosti vyžadování údajů od (potenciálního) zaměstnance před uzavřením pracovního poměru, § 248 odst. 2 věnující se kontrole věcí a prohlídek zaměstnanců, § 312 upravující osobní spis zaměstnance či § 313 až 315 upravující potvrzení o zaměstnání a pracovní posudek.[11]

Z hlediska zpracování osobních údajů je samozřejmě důležitý zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen „ZZOÚ"), ač tento předpis nebude do budoucna již výchozí normou pro zpracování osobních údajů, jak tomu bylo v případě jeho předchůdce, tj. v případě zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném do 23. dubna 2019 (dále jen „ZOOÚ"). ZZOÚ se totiž zaobírá spíše specifickými případy zpracování osobních údajů[12] a je spíše doplňkovým předpisem k nařízení GDPR. I přesto jde nepochybně o jeden z klíčových předpisů pro zpracování osobních údajů mimo jiné i z důvodu, že upravuje postavení a pravomoc ÚOOÚ.

Je-li předmětem této práce rovněž ochrana osobnosti, nelze ve výčtu národních pramenů samozřejmě opomenout zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „ObčZ"). Ten se o ochraně osobnosti zmiňuje hned ve svém prvním ustanovení (§ 1 odst. 2 ObčZ) zakotvujícím zásadu dispozitivnosti, která je limitována mimo jiné právě ochranou osobnosti a jejím porušením. Blíže se pak ochraně osobnosti věnují ustanovení § 81 a násl. ObčZ, které blíže upravují některé vybrané aspekty ochrany osobnosti člověka, ať už se jedná o podobu a soukromí, o práva na duševní a tělesnou integritu, či o ochranu lidského těla. Přestože se jedná o demonstrativní výčet, je

[11] Tento výčet není úplný. Zmínka o zpracování údajů zaměstnanců je dále obsažena v některých dalších ustanoveních (např. v ustanovení § 137 odst. 2 či § 150 ZPr).

[12] Jedná se zejména o zpracování osobních údajů příslušnými orgány za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech a zpracování osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky (srov. § 2 ZZOÚ).

relativně komplexní a těžko hledat další práva, která by v těchto ustanoveních již nebyla zmíněna.[13]

1.1.2 Další zákonné normy

Tři zákony zmíněné v předchozí kapitole jsou z hlediska předmětu této práce zcela zásadní, přesto však nelze opomenout celou řadu dalších právních předpisů, které mají rovněž vliv na ochranu osobních údajů, potažmo ochranu osobnosti, v pracovněprávních vztazích. Z hlediska předmětu této práce stojí za zmínku zejména následující předpisy: zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon), ve znění pozdějších předpisů, zákon č. 435/2004 Sb., zákon o zaměstnanosti, ve znění pozdějších předpisů (zejména § 12 a § 17), zákon č. 251/2005 Sb., o inspekci práce, ve znění pozdějších předpisů (zejm. § 11a a § 24a), zákon č. 251/2016 Sb., o některých přestupcích, ve znění pozdějších předpisů (§ 7), zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (§ 180 a násl.). Dále pak celá řada dalších předpisů, které vymezují předpoklady pro výkon určitých povolání a funkcí, když přímo či nepřímo určují rozsah osobních údajů,[14] které je zaměstnavatel oprávněn vyžadovat a dále uchovávat, které upravují specifická pravidla pro možnost kontroly zaměstnanců a jejich kontrolu,[15] které upravují možnost zpracování rodných čísel[16] apod.

1.1.3 Ústavní předpisy a ostatní právní normy

Při výkladu o ochraně osobnosti nelze opomenout skutečnost, že ochrana soukromí je zaručena národními předpisy nejvyšší právní síly. Listina základních práv a svobod (dále jen „LZPAS“) tyto upravuje v širším smyslu jako právo na ochranu soukromí, a to v článku 7 a v článku 10, v jejichž rámci je garantována ochrana nedotknutelnosti osoby a jejího soukromí, právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a na ochranu jména a rovněž právo na ochranu před neoprávněným shromažďováním, zveřejňováním

---

[13] V odborné literatuře bývá zmiňováno například právo na ochranu osobní svobody (srov. Tůma in Lavický, P. a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. Komentář. 1. vydání, Praha: C. H. Beck, 2014, s. 417.

[14] Např. zákon č. 451/1991 Sb., kterým se stanoví některé další předpoklady pro výkon některých funkcí ve státních orgánech a organizacích České a Slovenské Federativní Republiky, České republiky a Slovenské republiky, ve znění pozdějších předpisů.

[15] Např. zákon č. 234/2014 Sb., o státní službě, ve znění pozdějších předpisů, či zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, ve znění pozdějších předpisů.

[16] Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů.

nebo jiným zneužíváním osobních údajů. Případně též v článku 13 zakotvujícím listovní tajemství.

Určitá pravidla týkající se ochrany osobnosti či spíše zpracování osobních údajů ve specifických případech jsou k nalezení rovněž v podzákonných právních normách, ať už se jedná o vyhlášky ministerstev, či o nařízení vlády. Jde například o nařízení vlády č. 201/2010 Sb., o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu, ve znění pozdějších předpisů, nařízení vlády č. 145/2015 Sb., o opatřeních souvisejících s oznamováním podezření ze spáchání protiprávního jednání ve služebním úřadu, či vyhlášku č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu. Jak je z uvedených příkladů patrné, tyto normy upravují značná specifika, a proto jim nebude dále věnována pozornost.

1.2 Předpisy Evropské unie

Z hlediska důležitosti je bezpochyby nutné věnovat se po výkladu o národních pramenech evropským předpisům. Základní a nejjednodušší je dělit právo Evropské unie na primární, které je tvořeno především Smlouvou o Evropské unii a Smlouvou o fungování Evropské unie (dále též jako „SFEU"), a sekundární, které tvoří nařízení, směrnice, rozhodnutí doporučení a stanoviska.[17] Kromě toho právo Evropské unie dotváří rovněž relevantní judikatura Soudního dvora Evropské unie (resp. obecné zásady dovozované tímto soudním dvorem)[18] a bez významu nejsou ani doporučení nebo stanoviska či jiné obdobné dokumenty orgánů EU, ačkoliv ty již nejsou závazné (z hlediska této práce se jedná především o WP29). I těmto bude v této práci věnována pozornost.

1.2.1 Sekundární právo Evropské unie

Evropský parlament a Rada jsou oprávněny přijímat pravidla o ochraně osob při zpracování osobních údajů na základě čl. 16 odst. 2 SFEU. Toto zmocnění je přitom hojně využíváno a v sekundárním právu existuje celá řada právních norem, které se ochraně osobních údajů věnují.

Základem ochrany osobních údajů v právu EU je nařízení GDPR. Díky své plné závaznosti a přímé použitelnosti ve všech členských státech EU je nařízení GDPR svým významem a aplikovatelností rovnocenné národním předpisům. Jeho přijetím došlo ke

[17] Čl. 288 SFEU.
[18] Tomášek, M., Týč, V. a kol. *Právo Evropské unie*. 2. aktualizované vydání. Praha: Leges, 2017, s. 102.

zrušení Směrnice, která byla po více než dvacet let primárním zdrojem pravidel ochrany osobních údajů. Směrnice harmonizovala, či spíše sblížila právní předpisy na ochranu osobních údajů v členských státech EU a zavedla jejich volný pohyb v rámci EU. To vše navíc bylo podpořeno jednotným výkladem pravidel obsažených ve Směrnici ze strany Soudního dvora Evropské unie.[19] Směrnice nicméně již nadále neodpovídala rozvíjejícím se technologiím, nárůstu datových toků a možnostem zpracování osobních údajů v dnešní době. Vedle toho zamýšlená harmonizace nebyla úplná a v podstatě ve všech členských státech EU byla Směrnice implementována trochu odlišně. Proto došlo s účinností od 25. května 2018 ke zrušení Směrnice a jejímu nahrazení nařízením GDPR.

Nařízení GDPR a Směrnice nejsou jediné dva prameny sekundárního práva EU, které se zabývají problematikou osobních údajů. Z hlediska tématu disertační práce za zmínku stojí například nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů. Jak je z názvu patrné, věnuje se toto nařízení výhradně zpracování osobních údajů v rámci orgánů a institucí Evropského společenství a z hlediska svého obsahu (stanovenými pravidly) je velmi obdobné Směrnici a nařízení GDPR. Ochraně osobních údajů se dále věnují některé specifické směrnice,[20] ale ty již nejsou pro tuto práci relevantní.

1.2.2 Primární právo EU

Původní myšlenkou Evropského společenství nebylo ochraňovat lidská práva, a proto ani původní verze zakládajících smluv se lidským právům, potažmo ochraně osobnosti a osobních údajů, nevěnovaly. Soudní dvůr sice začlenil lidská práva mezi obecné zásady ve snaze více chránit občany EU, písemného sepsání se však těmto pravidlům dostalo až v roce 2000, a to v rámci Listiny základních práv Evropské unie (dále jen „LZPEU“). Ta byla sice původně jen nezávazným dokumentem, ale v roce 2009 se stala součástí primárního práva poté, co vstoupila v platnost tzv. Lisabonská smlouva.

---

[19] Respektive jeho předchůdce, kterým byl Evropský soudní dvůr.

[20] Například 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 o soukromí a elektronických komunikacích), směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES, nebo 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.

Pokud jde o ochranu osobnosti a osobních údajů, je v LZPEU důležitý zejména čl. 8. Ten každému zaručuje právo na ochranu osobních údajů, které se ho týkají. Ale neomezuje se jen na toto konstatování a ve svém odst. 2 ukládá subjektům zpracovávajícím údaje, aby tyto byly *„zpracovávány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem“*. Je přitom zajímavé, že v tomto ustanovení je jako právní základ vyzdvihován souhlas, což byl princip zavedený Směrnicí, ale v rámci nařízení GDPR byl již opuštěn.

Zároveň je každému garantováno právo na přístup ke zpracovávaným údajům a právo na opravu jejich opravu, a rovněž je stanoveno, že na dodržování těchto pravidel má dohlížet nezávislý orgán. Za pozornost stojí, že ochrana osobních údajů je v tomto dokumentu stanovena ve prospěch „každého“, za což lze považovat nejen fyzické, ale i právnické osoby. Obecně však platí, že veškerá další právní úprava ochrany osobních údajů (zejména nařízení GDPR či Směrnice) se věnuje pouze ochraně osobních údajů fyzických osob.[21]

Závěrem k článku 8 LZPEU stojí ještě za zmínku, že jde v podstatě o první a jediné zakotvení práva na ochranu osobních údajů do dokumentu tohoto typu. Toto právo totiž není známé ani z LZPAS ani z Evropské úmluvy o ochraně lidských právech (dále jen „EÚLP“). Rovněž svým vznikem bylo specifické, jelikož jen zakotvilo a podtrhlo principy, které byly již známy ze sekundárního práva, konkrétně ze Směrnice.

Z hlediska ochrany osobnosti stojí v rámci LZPEU za zmínku dále čl. 7, podle kterého má každý *„právo na respektování svého soukromého a rodinného života, obydlí a komunikace“*. Zejména pak ochrana soukromého života je z hlediska předmětu této práce důležitá, jelikož na pracovišti mnohdy dochází ke střetům tohoto práva s právem zaměstnavatele na kontrolu, resp. právem na ochranu jeho vlastnictví.

Při výkladu o primárním právu nelze opomenout zakládací smlouvy samotné. V rámci již zmiňovaného čl. 16 odst. 1 SFEU je každému garantováno *„právo na ochranu osobních údajů, které se jej týkají“*. I v tomto případě je tedy ochrana osobních údajů upravena ve prospěch „každého“, nejen vůči fyzickým osobám.

[21] Ochrana osobních údajů právnických osob přitom není koncept, který v rámci Evropské unie nebyl znám. Například rakouská právní úprava ochrany osobních údajů, kterou byla implementována Směrnice, ochranu osobních údajů právnických osob znala. Tato byla odstraněna až s nástupem nařízení GDPR.

1.2.3 Ostatní prameny

Z hlediska evropského práva není rozhodné jen primární a sekundární právo. Dalším významným pramenem evropského práva jsou obecné právní zásady, které jsou především dovozovány v rámci rozhodnutí Soudního dvora EU. V té souvislosti stojí za zmínku též samotná rozhodnutí této soudní instituce, která jsou sama o sobě významným nástrojem poznání evropského práva, zejména v rámci rozhodování o předběžných otázkách.[22] Mezi nejznámější rozhodnutí, která jsou v této práci dále zmíněna, patří zejména rozhodnutí SDEU C-101/01, ve věci Bodil Lindqvist, či C-131/12, ve věci Google Spain.

V souvislosti s výkladem o pramenech práva je vhodné zmínit se též o nezávazných dokumentech, které však mají značnou výkladovou váhu. Na poli ochrany osobních údajů jde především o výkladová stanoviska WP29.[23] Přestože měla WP29 jen poradní funkci, v mezidobí let 1997 až 2016 se stala uznávaným orgánem, který vydáním více než dvou set stanovisek, názorů, pracovních programů či jiných obdobných dokumentů významnou mírou přispěl k dotváření práva na ochranu osobních údajů. Z hlediska pracovních vztahů pak stojí za zmínku zejména stanovisko ze dne 13. září 2001 č. 8/2001 ke zpracování osobních údajů v pracovněprávním kontextu (WP48), pracovní dokument ze dne 29. května 2002 týkající se sledování elektronických komunikačních prostředků na pracoviště (WP55) či stanovisko ze dne 8. června 2017 týkající se zpracování údajů na pracovišti (WP249). Těmto a dalším dokumentům WP29 bude ostatně věnována odpovídající pozornost při výkladu o příslušných otázkách.

Ačkoliv WP29 spolu se zrušením Směrnice a účinností nařízení GDPR zanikla, neznamená to, že by její výklad nebyl již nadále relevantní. Nařízení GDPR totiž zavedlo tzv. Evropský sbor pro ochranu osobních údajů (dále jen „Sbor“), který v podstatě tuto WP29 nahrazuje.[24] Sbor přitom hned v první den své existence, tj. 25 května 2018, formálně potvrdil platnost vybraných stanovisek WP29[25] a formálně tak deklaroval kontinuitu práce.

---

[22] Tomášek, M., Týč, V. a kol. *Právo Evropské unie*. 2. aktualizované vydání. Praha: Leges, 2017, s. 390.
[23] Přestože WP29 v souvislosti s účinností nařízení GDPR zanikla, její stanoviska jsou s ohledem na podobnost nařízení GDPR se Směrnicí a jejich obecnost ve značné míře aplikovatelná i za účinnosti nařízení GDPR.
[24] Srov. preambule 139 a čl. 94 odst. 2 nařízení GDPR.
[25] Endorsement of GDPR WP29 guidelines by the EDPB. In edpb.europa.eu, 25. května 2018 [online]. [cit. 2018-11-15]. Dostupné z: https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_cs

1.3 Mezinárodní prameny

Při výkladu o právu na ochranu osobnosti jsou neopomenutelným pramenem práva též prameny mezinárodní. Tyto prameny mají již značný odstup od každodenního života zaměstnanců a jejich ochrany, nemají obvykle přímý dopad na samotné jedince a standardně jen zavazují členské státy příslušných mezinárodních organizací k dosažení určitých cílů. To však neplatí zcela pro Radu Evropy.

1.3.1 Rada Evropy

Rada Evropy je mezinárodní organizací, založenou již v roce 1949, a v současné době je jejím členem celkem 47 zemí. Od jejího založení byla na půdě Rady Evropy přijata celá řada úmluv, konvencí, doporučení protokolů či jiných obdobných dokumentů, přičemž bezpochyby nejdůležitější z nich je EÚLP, ke které se přihlásily všechny členské státy této organizace. EÚLP je zcela jedinečná především tím, že na její dodržování dohlíží Evropský soud pro lidská práva sídlící ve Štrasburku (dále jen „ESLP“). Tento se za dobu své existence vypořádal již s více než 800 tisíci stížností.[26] Existence tohoto soudu má tudíž značné dopady na faktické využití EÚLP ze strany jednotlivců a staví ji z tohoto hlediska nad jakékoliv jiné mezinárodní úmluvy. Jak je vysvětleno dále, EÚLP neopomíjí též ochranu soukromí zaměstnanců a nejednou se již stalo, že se zaměstnanec domohl svého práva až právě před ESLP.

Z hlediska ochrany osobnosti zaměstnanců je rozhodným předpisem čl. 8 odst. 1 EÚLP, podle kterého platí, že *„každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence“*. Význam tohoto ustanovení a jeho jednotlivých pojmů je přitom dále dovozován v judikatuře ESLP, jelikož EÚLP v tomto žádná bližší vodítka neposkytuje.

Při výkladu o EÚLP je vhodné se ještě zmínit o jejím vztahu s LZPEU. Při bližším zkoumání totiž vychází najevo, že práva přiznaná v EÚLP se značně shodují s právy LZPEU. Aplikační a výkladové problémy by pak teoreticky mohly nastat, pokud jsou pro určitý stát závazné oba dokumenty. Tomuto problému bylo nicméně předejito v rámci pozdějšího dokumentu, tj. LZPEU, v čl. 52 odst. 3, ve kterém se uvádí, že *„pokud tato listina obsahuje práva odpovídající právům zaručeným Úmluvou o ochraně lidských práv*

[26] The Council of Europe at 70: Milestones and achievements. In coe.int. 2 května 2019 [online]. [cit. 2019-05-07]. Dostupné z: https://www.coe.int/en/web/secretary-general/-/the-council-of-europe-at-70-milestones-and-achievements

a základních svobod, jsou smysl a rozsah těchto práv stejné jako ty, které jim přikládá uvedená úmluva. Toto ustanovení nebrání tomu, aby právo Unie poskytovalo širší ochranu.“. Tím je zajištěno, že výklad LZPEU bude vždy konzistentní s EÚLP, a zároveň není bráněno tomu, aby v rámci Evropské unie byla pomocí LZPEU přiznána širší ochrana, což je případ právě výslovné ochrany osobních údajů v již rozebíraném čl. 8 LZPEU.

Rada Evropy se však neomezuje jen na EÚLP. Za další dokument významný z hlediska ochrany osobních údajů a přijatý na půdě Rady Evropy je považována tzv. Úmluva č. 108 ze dne 28. ledna 1981,[27] o ochraně osob se zřetelem na automatizované zpracování osobních dat (dále jen „Úmluva 108“). Ze strany ÚOOÚ bývá dokonce označována za základní nadzákonný právní instrument.[28] V České republice s její ratifikací vyslovil souhlas Parlament České republiky v souladu s Ústavou České republiky a následně byla vyhlášena ve sbírce mezinárodních smluv pod č. 115/2001 Sb. m. s. a vstoupila v platnost dne 1. listopadu 2001, což z ní učinilo přímo použitelný předpis v České republice. Kromě toho byl Radou Evropy přijat též tzv. dodatkový protokol,[29] který Úmluvu č. 108 doplňuje a který byl v ČR vyhlášen pod č. 29/2005 Sb. m. s.

Jak může napovídat datum jejího přijetí, je Úmluva č. 108 již značně zastaralá, resp. stanovuje pouze velmi obecné závazky, které by příliš v praktickém životě subjektům údajů nepomohly.[30] To nezměnil ani zmiňovaný dodatkový protokol č. 181, který se zaměřuje především na povinnost zřídit orgán, který bude na ochranu osobních údajů dohlížet, a na předávání osobních údajů do třetích zemí. Právě z těchto důvodů není Úmluvě 108 v této práci věnována větší pozornost. Tuto skutečnost si nyní snad i uvědomuje Rada Evropy, neboť došlo na její půdě v loňském roce k rozhodnutí o její modernizaci.[31] Závěrem k Úmluvě 108 se ještě hodí poznamenat, že ačkoliv se závazků z ní vyplývajících nelze přímo domáhat před ESLP, byl to právě ESLP, který ve svých rozhodnutích označil ochranu osobních údajů za nedílnou součást práva na soukromí ve smyslu čl. 8 EÚLP.[32]

---

[27] Tento den má dopady do dnešní doby, jelikož datum 28. ledna je označováno za den ochrany osobních údajů.
[28] ÚOOÚ: *Rubrika Právní předpisy*. In uoou.cz [online]. [cit. 2018-11-16]. Dostupné z: https://www.uoou.cz/pravni-predpisy/ds-1257/p1=1257
[29] Plným názvem Dodatkový protokol č. 181 k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice.
[30] Nonnemann, F. *Modernizace Úmluvy 108, základního nástroje Rady Evropy pro ochranu osobních údajů.* In epravo.cz. 20. července 2018. [online]. [cit. 2019-01-11]. Dostupné z: https://www.epravo.cz/top/clanky/modernizace-umluvy-108-zakladniho-nastroje-rady-evropy-pro-ochranu-osobnich-udaju-107901.html
[31] 28 January – Data protection day. In coe.int. 28 ledna 2019 [online]. [cit. 2019-02-01]. Dostupné z: https://www.coe.int/bs/web/portal/28-january-data-protection-day
[32] Např. rozhodnutí ESLP ze dne 25. února 1997 ve věci Z. vs. Finsko, č. stížnosti 22009/93.

Tímto v podstatě povinnosti stanovené Úmluvou 108 nepřímo vztáhl do své rozhodovací působnosti.

Na půdě Rady Evropy vznikly i další dokumenty zajímavé z hlediska ochrany zaměstnanců či pracovněprávních vztahů. Za zmínku stojí zejména Evropská sociální charta,[33] která bývá spolu s EÚLP označována za jeden ze dvou základních pilířů ochrany lidských práv v působnosti Rady Evropy a za mezník při sjednocování sociálních politik.[34] Nicméně se nevěnuje ani ochraně osobnosti, ani ochraně osobních údajů. Tomuto tématu se naopak věnují některá doporučení přijatá Radou Evropy. Za zmínku stojí zejména doporučení z roku 2015 týkající se zpracování osobních údajů na pracovišti[35] nebo doporučení o ochraně osobních údajů využívaných pro potřeby zaměstnání.[36] Tato doporučení lze do určité míry připodobnit stanoviskům WP29, oproti nim se však problematikou nezaobírají v takové míře detailu, a proto nebudou dále v této práci zkoumány.

1.3.2 Ostatní prameny

Rada Evropy, ač mnohdy přesahuje svou činností geografické hranice Evropy,[37] neoslovuje a s největší pravděpodobností nikdy nebude oslovovat celý svět. V těchto měřítkách působí jiné organizace, přičemž z hlediska předmětu této práce má svůj nezpochybnitelný význam a úlohu Organizace spojených národů (dále jen „OSN“). Primární cílem této organizace přitom není jen podpora mezinárodního míru a bezpečnosti, poskytování humanitární pomoci, podpora ekonomického a sociálního rozvoje, ale rovněž i ochrana lidských práv. Z toho hlediska je klíčovým dokumentem Všeobecná deklarace lidských práv přijatá na Valném shromáždění OSN dne 10. prosince 1948 (dále jen „VDLP“).

---

[33] Ač byla přijatá už v roce 1961, nabyla Evropská sociální charta v ČR účinnosti až v roce 1999, a to v návaznosti na své vyhlášení pod č. 14/2000 Sb. m. s. Také Evropská sociální charta byla předmětem několika dodatkových a pozměňovacích protokolů.

[34] Tröster, P. *Právo sociálního zabezpečení.* 6. podstatně přepracované a aktualizované vydání. Praha: C. H. Beck, 2013. Academia iuris, s. 40.

[35] Doporučení Rady Evropy č. CM/Rec(2015)5 týkající se zpracování osobních údajů na pracovišti, ze dne 1. dubna 2015 [online]. [cit. 2018-11-10]. Dostupné z: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

[36] Doporučení Rady Evropy č. R (89) 2, o ochraně osobních údajů využívaných pro potřeby zaměstnání, ze dne 18. ledna 1989 [online]. [cit. 2018-11-10]. Dostupné z: https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf

[37] Například Úmluva č. 108 byla ratifikována a je účinná i pro řadu mimoevropských zemí, mezi které patří např. Uruguaj, Tunisko, Senegal nebo Mexiko.

Z hlediska ochrany osobnosti, potažmo soukromí, má význam především čl. 12 VDLP, podle kterého *„nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“*. Jde tedy v principu o shodnou zásadu, která je vyjádřena v čl. 8 EÚLP s tím drobným rozdílem, že v rámci VDLP je toto právo vyjádřeno negativně jako zákaz zasahování, kdežto v EÚLP je vyjádřeno jako právo na respektování vymezených aspektů života, obydlí a korespondence.

Ochrana osobních údajů v rámci VDLP výslovně zmíněna přirozeně není. S ohledem na dobu přijetí VDLP byl značný pokrok, že se vůbec podařilo mezi tolika členskými státy OSN[38] na deklaraci, kterou je VDLP, společně dohodnout. Na druhou stranu si lze klást otázku, zda by ji nebylo možné dovodit a vztáhnout pod ochranu soukromí v rámci zmiňovaného čl. 12, obdobně jak to dovodil ESLP ve vztahu k EÚLP. Autor této práce se domnívá, že není důvod, proč by toto nebylo možné dovodit, obzvláště s ohledem na změnu dnešního života a prudký rozvoj technologií. Lze tak dojít k závěru, že i ochrana osobních údajů své zakotvení v rámci VDLP má, byť nikoliv výslovné.

Na půdě OSN vznikly v této souvislosti ještě dva důležité dokumenty. Jedná se o Mezinárodní pakt o občanských a politických právech (dále jen „MPOPP“) a Mezinárodní pakt o hospodářských, sociálních a kulturních právech.[39] Jak je z názvu patrné, jedná se mezinárodní smlouvy, přičemž obě v podstatě plynule navazují na VDLP a na rozdíl od VDLP právně závazným způsobem stanovují povinnosti pro státy, které k těmto smlouvám přistoupí. MPOPP ve svém čl. 17 přitom totožně přejímá závazek k ochraně soukromí obsažený v čl. 12 VDLP.

V neposlední řadě lze říci, že v rámci OSN jsou též přijímána rozhodnutí, která se mohou týkat zpracování osobních údajů. Za zmínku stojí především rozhodnutí Valného shromáždění OSN ze dne 14. prosince 1990, kterým byly přijaty Pokyny ohledně právní úpravy počítačových souborů s osobními údaji.[40] Z takovýchto rozhodnutí přitom při svých rozhodnutích neváhá vycházet ani ESLP.[41]

---

[38] To platí, přestože v době přijetí VDLP bylo pouze 58 členů OSN. Dnes jich je 193.

[39] Tato mezinárodní úmluva obsahuje též mnoho práv na ochranu osobnosti, nejsou však relativní pro tuto práci.

[40] V originále označené jako „*Guidelines for the regulation of computerized personal data files*.“

[41] Srov. například rozhodnutí Velkého senátu ESLP ze dne 5. září 2017 ve věci Barbulescu vs. Rumunsko, č. stížnosti 61496/08.

Již od roku 1919 úzce navázala na činnost Společnosti národů tzv. Mezinárodní organizace práce (dále jen „MOP“), která se pak stala specializovanou organizací OSN. Zaměřuje se na vytvoření celosvětově platných standardů, pravidel, politik či programů pro důstojnou práci všech mužů a žen. Ty formuluje prostřednictvím úmluv, které se stávají závaznými po jejich ratifikaci členskými státy, či doporučení, která jsou, jak je z názvu patrné, nezávazná. Mají však obvykle význam pro výklad pravidel obsažených v úmluvách.

Dokumenty týkající se ochrany osobnosti a osobních údajů jsou na půdě MOP zatím vydávány pouze v nezávazné formě. Bezpochyby nejvýznamnější z nich je kodex Ochrana osobních údajů zaměstnanců.[42] Jeho účelem je poskytnout návod, jak zacházet s osobními údaji zaměstnanců a jak je ochraňovat. Jakožto nezávazný dokument se kodex snaží především vysvětlovat, co je dobrá praxe, poskytovat doporučení a má sloužit jako podklad pro zákonodárce při tvorbě příslušné legislativy, kolektivních smluv, vnitřních předpisů zaměstnavatelů apod. Přes jeho značný přínos ve své době je dnes na území Evropské unie už do značné míry překonán, a to závazným nařízením GDPR spolu s nezávaznými doporučeními WP29. Proto nebude v rámci této práce blíže zkoumán.

Kromě toho vydává MOP rovněž zvláštní pracovní dokumenty (v angličtině označovány jako „*working papers*“), které vznikají pro řešení konkrétních specifických otázek. Jako příklad lze uvést pracovní dokument z 5. června 2018 týkající se zpracování biometrických a dalších citlivých údajů pro potřeby sociálního zabezpečení.[43]

---

[42] International Labour Office (ILO). Code of Pracite: Protection of workers‘ personal data. Geneva, International Labour Office, 1997. ISBN 92-2-110329-3. [online]. [cit. 2019-04-19]. Dostupný z: https://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf

[43] Carmona, M. S. *Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection*. ESS – Working paper No. 59. International Labour Office (ILO). 5 června 2018 [online]. [cit. 2018-11-05]. Dostupné z: https://harvardlpr.com/wp-content/uploads/sites/20/2016/06/10.2_7_Rogers.pdf

2 Východiska ochrany osobnosti a osobních údajů

Než se rozbor této práce zaměří na specifika pracovněprávních vztahů, je nutné věnovat se alespoň zčásti též obecným teoretickým východiskům ochrany osobnosti a osobních údajů. Jak bylo nastíněno v předchozí kapitole, existuje celá řada předpisů, které zásady a pravidla ochrany osobnosti a ochrany osobních údajů upravují, a to na národní, mezinárodní či evropské úrovni. Cílem této kapitoly je podat ucelený přehled o obsahu těchto právních norem, tedy popsat východiska, která budou základem pro další výklad v této práci. To zahrnuje analýzu právního chápání těchto oblastí, jednotlivých jejich složek, způsoby ochrany, zčásti také z hlediska historického kontextu. Cílem této kapitoly je dále též popsat vzájemný vztah mezi ochranou osobnosti a ochranou osobních údajů, včetně analýzy shodných prvků a vzájemných odlišností těchto dvou právních oblastí.

2.1 Právo na ochranu osobnosti

Na úvod výkladu k právu na ochranu osobnosti je nutné vymezit si samotný pojem ochrany osobnosti, jeho obsah a jeho chápání. Knapp k pojmu ochrany osobnosti uvádí, že *„subjektivní občanské všeobecné osobnostní právo, resp. v jeho jednotném rámci subjektivní dílčí osobnostní práva lze definovat jako možnost každé fyzické osoby jako individuality a suveréna nakládat v mezích právního řádu podle svého uvážení co nejšíře se svou osobností, resp. s jednotlivými hodnotami tvořícími celistvost její osobnosti v její fyzické a morální jednotě vůči ostatním subjektům […] s rovným právním postavením za účelem její realizace ve společnosti, jakož i ochrany jejich zájmů, potřeb a preferencí“.*[44] Poněkud stručnější definici lze pak nalézt v učebnici občanského práva, která uvádí, že právem na ochranu osobnosti se rozumí „*jednotné právo, jehož účelem a obsahem je v občanskoprávní oblasti zabezpečit respektování osobnosti fyzické osoby a její všestranný svobodný rozvoj“.*[45]

Aniž by bylo snahou autora této práce hledat nejsprávnější definici tohoto pojmu, považuje za dostačující vymezení tohoto pojmu prostřednictvím jednotlivých charakteristických znaků. Klíčová pro pochopení je osobnost, potažmo osobní sféra jedince. Osobní sférou se osobnostní práva odlišují od práv majetkových, přičemž dělení na

[44] Knap, K., Švestka, J., Jehlička, O., Pavlík, P., Plecitý, V. *Ochrana osobnosti podle občanského práva*. 4., podstatně přeprac. a dopl. vyd. Praha: Linde, 2004. s. 92.
[45] Tichý, L. *Obecná část občanského práva*. V Praze: C. H. Beck, 2014. Právní praxe, s. 34.

osobnostní a majetková práva je jedním ze základních dělení subjektivních občanských práv. Telec v této souvislosti hovoří o dvou pilířích občanského práva, a to o osobnosti a vlastnictví.[46]

Charakteristikou osobnostních práv je, že se jedná o absolutní práva (tj. působí vůči všem, když určují povinnost kterékoliv osoby nekonat, resp. jiného nerušit ve výkonu svého práva).[47] To je velmi důležité pro chápání a porozumění tomu, jak právo na ochranu osobnosti zaměstnanců funguje, neboť toto právo primárně není o určování konkrétních povinností, nýbrž o určování pravidel nekonání určitým způsobem, který by se příčil osobnostním právům.[48] Jiným znakem těchto práv je, že jsou úzce spjata s konkrétní osobou a nepřechází na právní nástupce, jsou nepromlčitelná a příslušné právní normy upravující tato práva mají obvykle kogentní charakter.[49]

Obsahově je možné rozdělit právo na ochranu osobnosti na dvě složky, a to na pozitivní a negativní. Z hlediska právní ochrany je pak důležitá zejména složka negativní neboli zápůrčí, která již byla částečně zmíněna a která spočívá v povinnosti každého zdržet se zasahování do osobnostních práv jiného. Naopak složka pozitivní spočívá v oprávnění každého jednotlivce svobodně a dle své vůle jednat v souladu se svými osobnostními právy.[50] Z hlediska vztahů mezi zaměstnancem a zaměstnavatelem je pak důležitá především negativní složka, jelikož vztah zaměstnance a zaměstnavatele je nevyrovnaný, a o to více je důležité chránit zaměstnance a jeho osobnostní práva před zasahováním ze strany zaměstnavatele.

2.1.1 Ochrana osobnosti jako základní lidské právo

Jak bylo nastíněno v první kapitole, osobnostní práva jsou často ve své základní podobě zachycena v právních předpisech nejvyšší právní síly a v mezinárodních úmluvách či dokumentech věnujících se ochraně lidských práv. Mezinárodní základ těmto pramenům byl dán již po druhé světové válce v rámci VDLP, následně přijaté EÚLP a MPOPP

---

[46] Telec, I. *Přirozené právo osobnostní a jeho státní ochrana*. Právní rozhledy. 2007, 15(1), s. 5.
[47] Knap, K., Švestka, J., Jehlička, O., Pavlík, P., Plecitý, V. *Ochrana osobnosti podle občanského práva*. 4., podstatně přeprac. a dopl. vyd. Praha: Linde, 2004. s. 90.
[48] Existují však i relativní osobnostní práva, kdy se ochrana vztahuje pouze k vymezenému okruhu osob, tj. *inter partes*. Jde například o právo na odpověď a dodatečné sdělení, práva pacientů, ale i některá práva zaměstnanců (blíže srov. Tůma in Lavický, P. a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. Komentář. 1. vydání, Praha: C. H. Beck, 2014, s. 399-400).
[49] Srov. ustanovení § 1 odst. 2 ObčZ, podle kterého platí: „*Nezakazuje-li to zákon výslovně, mohou si osoby ujednat práva a povinnosti odchylně od zákona; zakázána jsou ujednání porušující dobré mravy, veřejný pořádek nebo právo týkající se postavení osob, včetně práva na ochranu osobnosti.*“
[50] Op. cit. sub. 46.

nebo Mezinárodního paktu o hospodářských, sociálních a kulturních právech. Přestože lze s nadsázkou říci, že tyto dokumenty byly brány na našem území v potaz až v devadesátých letech 20. století,[51] dnes je to už téměř 30 let, co tvoří nezpochybnitelnou součást našeho právního řádu, což je mimo jiné vyjádřeno i příslušnými ustanoveními LZPAS[52] a judikaturou Ústavního soudu ČR.[53]

Toto zakotvení dostatečně podtrhuje význam osobnostních práv, jejich přirozenoprávní charakter. Telec v této souvislosti uvádí, že *„mezi všemi subjektivními lidskými právy hraje přirozené právo osobnostní prvořadou roli. Bez života není vlastnictví a dokonce ani rodina.“.*[54] Obecně přitom platí, že osobnostní práva jsou jako přirozená práva každému vrozená (nezadatelná v nabytí) a trvale platná (nezadatelná v existenci).

K vymezení těchto práv je přitom možné dojít už pouhým rozumem, svědomím či vcítěním se, což je ostatně obecná vlastnost přirozených práv.[55] I z těchto důvodů stát obvykle přiznává těmto právům zvláštní ochranu, která zpravidla nespočívá jen v soukromoprávních nárocích (zejména žaloby na ochranu osobnosti), ale též v oblasti veřejného práva (zejména trestněprávní a správněprávní ochrana). Nezbytným předpokladem pro takovou ochranu je přitom podrobná úprava těchto práv, která je předmětem rozboru v následující podkapitole.

2.1.2 Ochrana osobnosti dle platné právní úpravy

Výše zmíněný přirozenoprávní charakter je podtržen v platné právní úpravě v rámci ObčZ. Důvodová zpráva k ObčZ pak správně vyzdvihuje ochranu osobnosti před vymezením právní subjektivity, když uvádí: „*Osobnost člověka se nechápe jako „přívěsek“ právní subjektivity, ale právní subjektivita je naopak pojata jako důsledek osobnosti člověka jako takového.“*[56] To je samo o sobě z podstaty důvodem, proč je výčet osobnostních práv v ObčZ jen demonstrativní, jelikož každý jednotlivý aspekt osobnosti a způsob její ochrany definovat nelze.[57]

---

[51] Tak například EÚLP byla v České republice vyhlášena až po její ratifikaci v roce 1992, a to v rámci sdělení č. 209/1992 Sb.
[52] Srov. čl. 10 LZPAS.
[53] Zejména nález Ústavního soudu ČR ze dne 18. dubna 1995, vyhlášený pod č. 55/1995 Sb., a ze dne 27. února 1997, vyhlášený pod č. 24/1997 Sb.
[54] Op. cit. sub. 46.
[55] Op. cit. sub. 46, s. 6.
[56] Poslanecká sněmovna ČR, Vláda ČR: Důvodová zpráva k zákonu č. 89/2012 Sb., občanský zákoník, a další související zákony (konsolidované znění), s. 63.
[57] S ohledem na zaměření této disertační práce je stranou ponechán bližší rozbor lidské osobnosti.

Výchozí premisa a závazek k ochraně osobnosti jsou v rámci ObčZ vyjádřeny v ustanovení § 3 odst. 2, podle kterého má každý *„právo na právo na ochranu svého života a zdraví, jakož i svobody, cti, důstojnosti a soukromí“*. Kromě toho je důležitost ochrany osobnosti zdůrazněna v již zmiňovaném § 1 odst. 2 ObčZ, který omezuje možnost upravovat si odchylně svá práva, pokud by ujednání osob porušovala mimo jiné i právo na ochranu osobnosti.

Základní materie ochrany osobnosti je následně obsažena v ustanoveních § 81 až 117 ObčZ. Z těchto ustanovení je nepochybně nejdůležitější generální klauzule ochrany osobnosti v rámci § 81 ObčZ. Ustanovení prvního odstavce uvádí, že je chráněna *„osobnost člověka včetně všech jeho přirozených práv. Každý je povinen ctít svobodné rozhodnutí člověka žít podle svého.“*. A podle druhého odstavce téhož ustanovení požívají ochrany *„zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy“*. Již těmito pouhými dvěma odstavci je v podstatě vyjádřeno vše dříve zmíněné, tedy že ochrana osobnosti je základním přirozeným právem, které je úzce spjato s osobností každého člověka, a že působí vůči všem. Zároveň je demonstrativně uveden výčet jednotlivých složek ochrany osobnosti. V dalších ustanoveních ObčZ jsou rozebírány způsoby ochrany pro případ zásahu do práv na ochranu soukromí. Následují vybrané složky ochrany osobnosti, kterými jsou podoba, soukromí, duševní a tělesná integrita, lidské tělo. Vedle toho existují i další složky osobnosti, která však blíže v ObčZ uvedeny nejsou, resp. nejsou zahrnuty přímo. Jde například o osobní svobodu, svobodu myšlení, zákaz nelidského zacházení či zákaz diskriminace (nicméně spadají pod ochranu důstojnosti).[58]

ObčZ však není jediným právním předpisem, který upravuje ochranu osobnosti. Kromě pramenů, které mají význam z hlediska předmětu této práce a o kterých bylo pojednáno v předchozí kapitole, je z hlediska ochrany osobnosti možné zmínit například zákon č. 46/2000 Sb., tiskový zákon, ve znění pozdějších předpisů a zákon č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, ve znění pozdějších předpisů, které obsahují právo na odpověď a právo na uveřejnění dodatečného sdělení. Z hlediska ochrany osobních údajů to dále může být například zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů, pokud jde o prostředí informační společnosti, zákon č. 21/1992 Sb., o bankách, ve znění

[58] Tůma in Lavický, P. a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. Komentář. 1. vydání, Praha: C. H. Beck, 2014, s. 418 a násl.

pozdějších předpisů, pokud jde o ochranu osobních údajů klientů, a celá řada dalších předpisů.

2.1.3 Možnosti ochrany osobnostních práv

Možností, jak se domáhat osobnostních práv, je celá řada. Teorie je dělí například na obecné a zvláštní prostředky.[59] Za obecné lze označovat přitom takové prostředky, které lze využít i v jiných oblastech práva mimo ochranu osobnosti. Může jít například o dohodu, svépomoc (§ 14 ObčZ), ochranu poskytovanou orgány veřejné správy či soudy. Naopak ochrana zvláštní je specifická právě pro ochranu osobnosti. Jde v podstatě o zvláštní soudní ochranu, kdy se lze u soudu domáhat svých práv prostřednictvím zvláštních žaloby.[60]

Tato právní úprava má své zakotvení v ustanovení § 82 ObčZ a na rozdíl od předchozí právní úpravy je tam uvedený výčet taxativním.[61] Jedná se o dva specifické nároky, kterých se lze domáhat prostřednictvím žalob, a to nárok zápůrčí a nárok odstraňovací. Žalobou zápůrčí se bude navrhovatel vždy domáhat toho, aby nějaké jednání rušitele bylo zakázáno nebo aby mu bylo uloženo, aby se takového jednání zdržel. Naopak žalobou odstraňovací se bude navrhovatel domáhat toho, aby došlo k odstranění následků způsobených zásahem do práva na ochranu osobnosti a obnovení předchozího právního stavu. Z hlediska předmětu této práce je obvyklé zejména uplatňování nároku odstraňovacího, jelikož ve vztahu mezi zaměstnancem a zaměstnavatelem k němu dochází zpravidla v případě vzniku sporu, kdy se zaměstnanec domáhá odstranění určitých následků, nicméně do úvahy připadá samozřejmě i uplatňování nároku zápůrčího. Důležité rovněž je, že oba tyto zmiňované nároky lze uplatnit kumulativně.

Přestože se jedná o úplný výčet zvláštních nároků vyplývajících z osobnostního práva, jak již bylo naznačeno, je možné se domáhat i dalších obecných nároků. V úvahu je třeba vzít zejména nárok na náhradu škody[62] či nemajetkové újmy a nárok na vydání bezdůvodného obohacení.[63] Důležitým odlišujícím prvkem výše zmíněných zvláštních

---

[59] Knap, K., Švestka, J., Jehlička, O., Pavlík, P., Plecitý, V. *Ochrana osobnosti podle občanského práva*. 4., podstatně přeprac. a dopl. vyd. Praha: Linde, 2004, s. 171.
[60] Švaňhal, R. *Ochrana osobnosti fyzický osob*. Právní rozhledy. 2000, 9, s. 385.
[61] Výčet prostředků ochrany v rámci ustanovení § 13 odst. 1 zákona č. 40/1964 Sb., občanský zákoník, ve znění účinném do 31. prosince 2013, byl naopak demonstrativní a bylo dovozeno, že se lze domáhat též jiných nároků.
[62] Zejména podle § 2894 a násl. ObčZ. Pro zásahu do přirozených práv člověka se přitom pro určení náhrady použije § 2956 ObčZ.
[63] Vyloučeno není ani uplatnění jiných obecných nároků, jako je například domáhání se svého práva pomocí určovací žaloby ve smyslu § 80 zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

nároků však je, že obecné nároky jsou založeny na subjektivní odpovědnosti, kdežto nároky osobnostní jsou založeny na konceptu odpovědnosti objektivní.[64]

Specifikem vzniku nároků z ochrany osobnosti je skutečnost, že jejich předpokladem nemusí být způsobení újmy. Přesto je v teorii obvykle dovozováno, že jednání škůdce musí mít alespoň způsobilost újmu přivodit. S ohledem na to je přitom možné dělit jednotlivé delikty proti právu na ochranu osobnosti na ohrožující a porušující. Toto je velmi důležité též pro vztah mezi zaměstnancem a zaměstnavatelem, protože při domáhání se svých práv z ochrany osobnosti, zejména soukromí, nemusí být na pracovišti vždy jednoduché konkrétní újmu určit.[65]

S ohledem na zaměření této práce je ještě nutné k výkladu o možnostech ochrany osobnostních práv zhodnotit praktické možnosti postupu zaměstnance v případě, že bude mít pocit, že dochází k zásahu do jeho práva na ochranu soukromí. Výše uvedený postup, kdy se zaměstnanec bude svých práv domáhat u soudu, nemusí být vždy rychlý, a tudíž efektivní (v pracovních sporech v roce 2015 činila průměrná délka řízení 602 dnů).[66] Soudy jsou jednoduše přehlcené, a když už se některé pracovněprávní spory dostanou před soud, obvykle se jedná o řízení týkající se určení neplatnosti ukončení pracovního vztahu. Sporů, které se týkají zásahu do práva na ochranu osobnosti, je naprosté minimum.[67] Toto je samozřejmě dlouhodobě neúnosné, avšak dokud nebude přijato legislativně a systémově jiné řešení, je nutné hledat jiné cesty, jak se svých práv domoci. Jak bude v této práci dále vysvětleno, také ZPr obsahuje určitá relevantní ustanovení, která slouží k ochraně osobnostních práv zaměstnance. K dohledu nad dodržováním těchto povinností jsou dle zákona č. 251/2005 Sb., o inspekci práce (dále jen „ZoIP“), povolány orgány inspekce práce.

Orgány inspekce práce mohou v první řadě poskytovat zaměstnavatelům a zaměstnancům bezúplatně základní informace a poradenství týkající se ochrany pracovních vztahů a pracovních podmínek (§ 5 odst. 1 písm. k) ZoIP). Zajímavější však je možnost podat podnět k zahájení kontroly, pokud bude mít zaměstnanec pocit, že je do jeho práva na ochranu osobnosti a soukromí zasahováno. Na základě takových kontrol mohou

---

[64] MELZER, Filip. *Občanský zákoník: velký komentář*. Svazek I. § 1-117. 1. vyd. Praha: Leges, 2013, s 525.
[65] Tůma in Lavický, P. a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. Komentář. 1. vydání, Praha: C. H. Beck, 2014, s. 471.
[66] Pichrt, J. *Alternativní řešení pracovněprávních sporů – strašák současnosti či naděje budoucnosti?* Sborník příspěvků z mezinárodní konference Pracovní právo 2016 na téma Zákoník práce v novelizaci, důchodová reforma v akci. Masarykova Univerzita, 2017.
[67] Přednášky účastníků na konferenci Nové příležitosti a meze uplatnění alternativních řešení sporů v České republice, konané dne 4. a 5. listopadu 2016, na Právnické fakultě Univerzity Karlovy.

být následně uložena opatření k odstranění nedostatků zjištěných při kontrole s určením přiměřené lhůty k jejich odstranění. Mohou rovněž navrhovat potřebná technická a jiná opatření k odstranění rizik, mohou být též samozřejmě ukládány sankce. To vše se přitom vztahuje i k porušení ustanovení, která v rámci ZPr chrání soukromí zaměstnanců (ač tomu tak dlouho nebylo).[68]

2.1.4 Složky práva na ochranu osobnosti

Ochrana osobnosti je velmi široký pojem a je možné ji rozdělit na celou řadu složek a podsložek. Je přitom chybné hovořit o tom, že by existovala absolutní osobnostní práva, ale jde o jednotné právo na ochranu osobnosti, jehož cílem je v rámci soukromoprávních vztahů *„zabezpečit respektování osobnosti člověka a jeho všestranný svobodný rozvoj“.*[69] Toto je patrné již z generální klauzule uvedené v § 81 ObčZ, která zakotvuje obecnou ochranu a jen demonstrativně uvádí některé složky ochrany osobnosti, která zákonodárce považoval za natolik důležité, aby je výslovně zmínil.

V teorii[70] se při dělení práva na ochranu osobnosti rozlišují nejčastěji následující složky: život, zdraví, čest, důstojnost, soukromí či projevy osobní povahy[71]. Vyjdeme-li z ustanovení § 81 ObčZ, je dále nutné do výčtu přidat *vážnost*, která je úzce spjata se ctí. Tyto pojmy nejsou dále blíže jasněji definovány,[72] přesto jsou jedním z nejčastějších předmětů sporů a žalob na ochranu osobnosti.[73] Dále ustanovení § 81 ObčZ obsahuje též právo na příznivé životní prostředí, které je mezi složky práva na ochranu osobnosti řazeno stále častěji v souvislosti se znečištěním životního prostředí a snahou tomu předcházet. Nicméně platí, že cílem této složky není ochraňovat přírodu jako takovou (to má na starosti veřejnoprávní regulace ochrany životního prostředí), nýbrž jen zdraví a tělesnou integritu člověka jako takového.

Tímto výčet jednotlivých složek a podsložek práva na ochranu osobnosti ale není vyčerpán. Dále je možné uvést jako příklad samotnou osobnost člověka, zákaz mučení a jiného nelidského zacházení, zákaz diskriminace, svobodu člověka, svobodu myšlení,

---

[68] Teprve v roce 2017 byla zákonem č. 206/2017 Sb., byla rozšířena působnost orgánů inspekce i na tuto oblast tím, že byl definován nový přestupek na úseku ochrany soukromí a osobních práv zaměstnanců (§11a a 24a ZoIP).
[69] Tůma in Lavický, P. a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. Komentář. 1. vydání, Praha: C. H. Beck, 2014, s. 392.
[70] Telec, I. *Chráněné statky osobnostní.* Právní rozhledy. 2007, 15(8), s. 272.
[71] Projevy osobní povahy zahrnují přitom i výtvory a díla, která jsou předmětem ochrany práva duševního vlastnictví.
[72] Ostatně jako i ostatní složky práva na ochranu osobnosti.
[73] Op. cit. sub. 69.

ochranu jména a podoby či ochranu osobních údajů. Telec v této souvislosti poukazuje dokonce na některé specifické složky, jako jsou osobní bezpečnost, osobní (nikoliv obchodní) tajemství, osobní podpis, osobní pracovní síla, osobní informovanost, osobní výchova a vzdělání či světonázorové sebeurčení.[74]

Jak je z úvodu patrné, záměrem této práce není věnovat se veškerým těmto složkám, ale jen těm, které souvisejí se vztahem zaměstnance a zaměstnavatele na pracovišti a s ochranou osobních projevů a ochranou soukromí. Stranou jsou pak ponechány jiné složky ochrany osobnosti, které by jinak mohly být pro vztah na pracovišti relevantní, jako je zákaz nucené práce, zákaz diskriminace apod.

2.1.5 Limitace práva na ochranu osobnosti

Tak jako každé lidské právo, naráží i právo na ochranu osobnosti na své limity. To se děje ve dvou rovinách. První rovina spočívá v zákonem aprobovaném omezení ochrany osobnosti a druhá rovina je představována střetem s ostatními právy (jiných osob).

Pokud jde o explicitně stanovené omezení, je pro jejich ústavnost důležité, aby byla stanovena zákonem.[75] V rámci ZPr lze jako typický příklad uvést ustanovení § 316 odst. 2 ZPr. Vedle toho je rovněž třeba, aby byly dodržovány ústavněprávní limity, jsou-li stanoveny. Ochrana osobnosti upravená v LZPAS však příliš takovýchto limitů nenabízí. Za zmínku stojí například čl. 12 odst. 2 a 3 LZPAS,[76] které se však netýkají složek ochrany osobnosti zkoumaných v této práci. V rámci českého právního řádu bude proto nutné vystačit si s obecnými premisami ochrany ústavních práv, vyplývajících především z obecných ustanovení (čl. 1 až 4) LZPAS. Určité specifické limitační pravidlo pro ochranu osobnosti týkající se soukromí nabízí EÚLP v čl. 8 odst. 2,[77] týká se však ochrany před svévolí státních orgánů definováním určitých konkrétních legitimních důvodů, jako jsou národní a veřejná bezpečnost, hospodářský blahobyt, ochrana pořádku atd. Ani LZPEU

---

[74] Op. cit. sub. 70.

[75] Srov. čl. 4 odst. 2 LZPAS. Rovněž stojí za zmínku, že taková zákonná omezení je nutné vykládat spíše restriktivně (srov. čl. 4 odst. 4 LZPAS).

[76] Podle čl. 12 odst. 3 LZPAS platí, že *„jiné zásahy do nedotknutelnosti obydlí mohou být zákonem dovoleny, jen je-li to v demokratické společnosti nezbytné pro ochranu života nebo zdraví osob, pro ochranu práv a svobod druhých anebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku. Pokud je obydlí užíváno také pro podnikání nebo provozování jiné hospodářské činnosti, mohou být takové zásahy zákonem dovoleny, též je-li to nezbytné pro plnění úkolů veřejné správy.“*

[77] Podle tohoto ustanovení platí, že *„státní orgán nemůže do výkonu tohoto práva [tj. práva na respektování rodinného a soukromého života] zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.“*

nemá vlastní specifické limitační pravidlo pro ochranu osobnosti, nabízí však pravidlo uplatňující se na veškerá práva LZPEU v obsažená. Podle toho pravidla platí, že *„každé omezení výkonu práv a svobod uznaných touto listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.“*. V tomto ustanovení jsou tedy zmíněny přinejmenším dva legitimní důvody omezení, a to cíle obecného zájmu a ochrana práv a svobod jiných.

Plynule lze tak navázat s výkladem o druhé rovině omezení ochrany osobnosti, kterou je proporcionalita mezi více právy, resp. různými právy různých osob. Tento princip vyplývá z čl. 4 odst. 4 LZPAS a je rovněž formulován v soudní praxí, a to národní i mezinárodní úrovni.[78] V České republice stojí za zmínku zejména nález Ústavního soudu ČR ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94, kde Ústavní soud dovodil: *„K omezení základních práv či svobod, i když jejich ústavní úprava omezení nepředpokládá, může dojít v případě jejich kolize. V těchto situacích je nutné stanovit podmínky, za splnění kterých má prioritu jedno základní právo či svoboda, a za splnění kterých jiné. Základní je v této souvislosti maxima, podle které základní právo či svobodu lze omezit pouze v zájmu jiného základního práva či svobody.“*[79]

Na pracovišti se bude nejčastěji jednat na střet práva na ochranu osobnosti a soukromí zaměstnance (čl. 10 LZPAS) a práva zaměstnavatele na ochranu jeho majetku (čl. 11 odst. 1 LZPAS). Správné posouzení této otázky je mnohdy naprosto klíčové pro posouzení legálnosti zásahů do ochrany soukromí zaměstnance. Z hlediska předmětu této práce lze v této souvislosti zmínit například rozhodnutí Ústavního soudu ČR ze dne 7. listopadu 2012, sp. zn. I. ÚS 3933/12, kterým byla odmítnuta stížnost proti rozhodnutí známému jako Kasalova pila[80] a kde Ústavní soud konstatoval, že *„právě míra zásahu do práva na soukromí stěžovatele kolidujícího s právem na ochranu majetku zaměstnavatele je pro rozhodování Ústavního soudu rozhodná“*.

Odpovědět přitom na otázku, které právo má kdy převážit, není vůbec jednoduché. Neexistuje na to ani žádný jednoduchý klíč, podle kterého by bylo možné vždy určit

[78] Bartoň, M., Kratochvíl, J., Kopa, M., Tomoszek, M., Jirásek, J., Svaček, O. *Základní práva*. Praha: Leges, 2016. Student, s. 95.
[79] Nález je publikován ve Sbírce zákonů pod č. 214/19934 Sb.
[80] Rozhodnutí Nejvyššího soudu ČR ze dne 16. srpna 2012, sp zn. 21 Cdo 1771/2011. Blíže k rozhodnutí srov bod 8.1.3.

převažující právo. Především bude vždy záležet na konkrétních skutkových okolnostech toho kterého případu. Ústavní soud ČR ve snaze toto alespoň trochu zformalizovat využívá tzv. třístupňový test, kdy jsou postupně hodnocena tři kritéria. Těmito kritérii jsou vhodnost (odpovídá na otázku, zda je omezením možné dosáhnout sledovaného legitimního cíle), nezbytnost (odpovídá na otázku, zda nejde sledovaného cíle dosáhnout jiným způsobem, kdy by nedocházelo k zásahu do lidského práva) a porovnání závažnosti obou v kolizi stojících práv, tj. přiměřenost v užším smyslu (odpovídá na otázku, zda újma na základním právu není nepřiměřená s ohledem na sledovaný legitimní cíl).[81]

Je otázkou, do jaké míry je toto skutečně vodítkem, když Ústavní soud dále dodává, že porovnávání závažnosti dvou práv pak spočívá *„ve zvažování empirických, systémových, kontextových i hodnotových argumentů“*.[82] Hledání takových argumentů přitom nebude snadné pro zkušeného právníka, natož pro osobu práva neznalou, a to i přesto, že Ústavní soud dále podává, v čem by tyto argumenty měly spočívat.

Závěrem lze nicméně shrnout, že ochrany své osobnosti a svého soukromí se mohou domáhat nejen osoby znalé testů proporcionality a mající zkušenosti s různými kategoriemi argumentů, jak je definuje Ústavní soud. Právo na ochranu osobnosti je přirozeným právem a to samo o sobě znamená, že základní prvky tohoto práva jsou zakotveny v každém z nás, stát toto právo pouze deklaruje, ale nekonstituuje.[83] Samozřejmě je ovlivňují různé společenské, kulturní i jiné aspekty. To platí shodně též pro jiná práva, včetně ochrany vlastnictví (majetku zaměstnavatele). V každém jsou zakotveny určité základy tohoto druhého práva, včetně znalosti zákazu odcizení či přivlastnění si majetku jiného. Každý si proto dokáže vnitřně sám vyhodnotit dvě proti sobě stojící práva a rozhodnout se, které převažuje. Zda bude rozhodnutí jedince „správné“, bude přitom vždy možné nechat soudně přezkoumat.

2.2 Ochrana soukromí

Záměrem této podkapitoly je blíže popsat pojem soukromí, a to z obecného hlediska a také z hlediska předmětu této práce. Vysvětlen je obsah pojmu soukromí a zkoumány jsou jednotlivé složky ochrany soukromí. V této souvislosti je též brán zřetel na historický vývoj tohoto pojmu a jeho obsahovou změnu v několika posledních letech způsobenou prudkým

[81] Srov. již citovaný nález Ústavního soudu ČR ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94.
[82] Tamtéž.
[83] Op. cit. sub. 78, s. 30.

rozvojem technologií a s tím spojenou publicizací soukromí, ať už dobrovolnou (vědomím zveřejňováním informací o svém soukromí), či nedobrovolnou (prostřednictvím nedovoleného zásahu třetích stran do soukromí jiných osob).

2.2.1 Pojem a podsložky ochrany soukromí

Tak jako ostatní složky ochrany osobnosti, je i pojem soukromí velmi neurčitý a jeho jednoznačná definice neexistuje. Pojem „soukromí" je záměrně zvolený obecný pojem, jehož smyslem je chránit soukromí, ať se daná osoba nachází kdekoliv. Může to být v obydlí, na pracovišti, ba dokonce a se svými limity na veřejnosti.[84] V zahraničí se někdy hovoří o teorii balónu či magnetického pole, která spočívá v tom, že každý jedinec má kolem sebe jakési pole či je v jakémsi balónu, který vždy jednotlivce doprovází a jehož velikost se mění v závislosti na interakci s jinými (větší balón a sdílený prostor s rodinou, naopak menší balón a více chráněné soukromí s cizími osobami).[85] Je nepochybné, že bližší obsah a konkrétní výklad tohoto pojmu se bude měnit s ohledem na historický, kulturní, hodnotový a společenský kontext. To v poslední době potvrzuje judikatura, která tento pojem vzhledem k celospolečenským změnám a rozvoji technologií neustále rozšiřuje. Přesto se mnoho autorů snaží tento pojem definovat.

Janečková a Bartík chápou soukromí jako určitou oblast života člověka, do které nemůže nikdo zasahovat bez výslovného zákonného zmocnění a bez souhlasu osoby, které se údaje týkají.[86] Dále přiznávají každému jedinci právo tuto sféru před každým tajit a ochraňovat, přičemž nikomu není dovoleno bez souhlasu oprávněného tuto oblast života narušovat. O podobnou definici pomocí definování možného chování podává Tůma, když uvádí: *„Součástí práva na ochranu soukromí je především možnost vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti osobního soukromí člověka zpřístupněny jiným subjektům."*[87] Naopak o přímou definici se pokusil ÚOOÚ, když uvedl, že jde o *„osobní, intimní sféru člověka v jeho integritě, která zahrnuje všechny projevy osobnosti konkrétního a jedinečného lidského tvora. Pojem soukromí obsahuje rovněž*

---

[84] Tak například Městský soud v Brně dovodil, že i „*prostory mimo obydlí se považují za soukromé prostory*" (srov. rozhodnutí Městského soudu v Brně ze dne 28. února 2007, sp. zn. 7 Ca 204/2005).
[85] Yanisky-Ravid, S. *To Read Or Not to Read: Privacy within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory*. American University Law Review, Vol. 64, No. 1, 2014, s. 83-84 [online]. [cit. 2019-02-01]. Dostupné z: https://ssrn.com/abstract=2231694
[86] Janečková, E. a Bartík, V. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde Praha, 2011, s. 43-46.
[87] Tůma in Lavický, P. a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. Komentář. 1. vydání, Praha: C. H. Beck, 2014, s. 444.

hmotný i myšlenkový prostor jednotlivce, součástí soukromého života je i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.“.[88]

Z uvedeného je zřejmé, že soukromí by bylo možné definovat pozitivní a negativní složkou. Pozitivní spočívá ve svobodě každého nakládat se svými soukromím a souvisejícími informacemi dle svého vlastního uvážení (například rozhodnout o utajení či zveřejnění příslušných informací). Negativní aspekt pak spočívá v možnosti ochrany před rušitelem soukromí a nároku na to, aby nikdo jiný do soukromí nezasahoval, aniž by to bylo povoleno zákonem, nebo k tomu dal daný subjekt svůj souhlas.[89]

Právo na ochranu soukromí má mnoho podsložek. Zejména zahrnuje právo na soukromí a rodinný život. Ochrana soukromého života přitom může spočívat ve fyzickém soukromí (integritě) a zásazích do něj nebo v soukromí nehmotném, spočívajícím především v ochraně informací o dané osobě. Právě tato ochrana informací či údajů o konkrétní osobě pak odpovídá veřejnoprávní ochraně osobních údajů, jak je upravena nařízením GDPR. Dále mohou být pod ochranu soukromí zařazeny písemnosti osobní povahy a ochrana soukromí pak úzce souvisí s ochranou listovního tajemství, jehož ochrana vychází z ústavního zakotvení v rámci čl. 13 LZPAS. Ochrana podoby a obrazových či zvukových záznamů týkajících se fyzické osoby jsou dalšími podsložkami ochrany soukromí. Tyto pak úzce souvisí s nejrůznějšími projevy osobní povahy.[90]

2.2.2 Vývoj ochrany soukromí

Pro úplné pochopení pojmu ochrany soukromí je vhodné učinit malý historický exkurz ke vzniku tohoto práva. Prapůvod ochrany soukromí lze identifikovat již několik století před Kristem, v době vzniku tzv. Hippokratovy přísahy, která mimo jiné dává základ k povinnosti mlčenlivosti o zdravotním stavu.[91] Bez ohledu na to se ochrana soukromí svého rozpracování dočkala až mnoho století poté v rámci common law, zejména v rozhodovací praxi soudů. Za první významnější rozhodnutí lze označit rozhodnutí vydané v rámci

[88] Stanovisko ÚOOÚ č. 6/2009: *Ochrana soukromí při zpracování osobních údajů*. Listopad 2009, aktualizace únor 2014.
[89] Op. cit. sub. 86.
[90] Wagnerová, E. *Právo na soukromí: Kde má být svoboda, tam musí být soukromí*, In. Šimíček, V. (ed.). *Právo na soukromí*. 1. vyd. Brno: Masarykova univerzita, 2011, s. 52 a násl.
[91] Srov. příslušnou část, která uvádí: „*Cokoli, co při léčbě i mimo svou praxi ve styku s lidmi uvidím a uslyším, co se nesmí sdělit, to zamlčím a uchovám v tajnosti.*“

tzv. Semayne's case z roku 1604, kdy byla vyjádřena zásada, podle které je pro každého jeho dům hradem a pevností.[92]

Dále došlo v 18. století na území Anglie k vydání dalších rozhodnutí,[93] avšak k důslednému rozpracování soukromí došlo až na americké půdě. Jak uvádí Seltenreich, byla to právě americká doktrína a judikatura, které se historicky na rozpracování práva na soukromí, resp. right to privacy, podílely nejvíce.[94] Základ ochraně soukromí položila americká ústava, konkrétně její čtvrtý dodatek, který se stal její součástí v roce 1792 a který garantoval všem jednotlivcům právo na ochranu svobody osobní a domovní a omezil možnost vydávání soudních příkazů, aniž by existovaly pádné důvody pro jejich vydání.[95] Za jeden z nejvýznamnějších doktrinálních počinů lze následně považovat článek Warrena a Brandeise v rámci Harvard Law Review z roku 1890. Byli to právě Warren a Brandeis, kteří položili slavnou definici soukromí jako práva být ponechán o samotě.[96] Tento článek se stal inspirací (a citačním zdrojem) pro následný judikaturní i legislativní rozvoj na území Spojených států amerických.

Bez ohledu na výše zmíněné neměla ochrana soukromí na americké půdě nikdy snadnou pozici. V první polovině 20. století začaly ve Spojených státech amerických vznikat různé policejní a vyšetřovací orgány a agentury, které měly s rozvojem technologií prakticky neomezené možnosti. Nejprve šlo o vznik FBI (1908), následoval vznik CIA (1947) a posléze došlo též ke vzniku dnes s ochranou soukromí nechvalně spojované NSA (1952). Fakticky tak došlo k tomu, že ochrana soukromí se mohla daleko lépe rozvíjet na území Evropy, kde byly klíčovými kroky již zmiňované přijetí EÚLP a následně i MPOPPP. Uvedenému nezabránilo ani přijetí tzv. Privacy Act v USA v roce 1974, naopak ochranu soukromí ještě více přibrzdilo přijetí tzv. Patriot Act. Dnes v důsledku všech těchto aspektů a v návaznosti na závažnější a závažnější prohřešky[97] hledá Amerika, jak se dotáhnout na evropskou regulaci představovanou nařízením GDPR.

---

[92] Solove, D. J., Schwartz, P. M. *Privacy Law Fundamentals*, Portsmouth: International Association of Privacy Professionals, 2017, s. 38.
[93] Např. rozhodnutí ze dne 6. prosince 1763 ve věci *Wilkes v. Wood*, podle kterého se poškozený (politik) úspěšně domáhal odškodnění za to, že jeho majetek byl prohledán, aniž by k tomu existovaly pádné důvody a byl řádně vydán soudní příkaz (op cit. sub 92).
[94] Seltenreich, R. *Právo na soukromí v kontextu ústavního vývoje USA*. Právník. 2000, 139(1), s. 23-26.
[95] Tamtéž.
[96] V orig. „*right to be let alone*", srov. Warren S. D., Brandeis L. D. *The Right to Privacy*. Harvard Law Review. 1890, Vol. 4, No. 5, s. 193.
[97] Za zmínku stojí například případ společnosti Cambridge Analytica, která zneužila údaje řádově miliónů uživatelů sociální sítě Facebook v rámci volebních kampaní v několika různých zemích.

Na závěr stojí ještě za zmínku, že americká doktrína definuje oblasti, kterých se tamní *privacy law* týká. Jedná se o vynucování práva (odposlechy a sledování), národní bezpečnost, zdravotní a genetické informace (zdravotnická mlčenlivost a genetické soukromí), vládní rejstříky (veřejné rejstříky a zveřejňování a přístup k informacím), finanční soukromí (bankovní tajemství, úvěrové registry), spotřebitelské údaje a obchodní záznamy (spam, spyware, soukromí telekomunikací, použití SSN,[98] přístup k PC, záznamy kamer atd.), bezpečnost dat (krádež identity, ohlašování případů poručení zabezpečení), soukromí ve školách a zaměstnání (osobní údaje státních zaměstnanců, limitace dotazování se při pohovorech).[99]

2.2.3 Ochrana soukromí v rozhodnutích soudů

Právo na ochranu soukromí je hojně interpretováno soudy, ať už na národní, či mezinárodní úrovni. O tom také svědčí bohatá judikatura na toto téma. Obvykle jde přitom o rozhodnutí soudů, které jsou na vrcholu soudních soustav a kterým obvykle přísluší výklad právních předpisů nejvyšší právní síly a v nich obsažených principů, kterým je i právo na ochranu soukromí.

V rámci národních dokumentů je bezpochyby nejdůležitější judikatura Ústavního soudu ČR. Jeho asi nejčastěji citované rozhodnutí, na které samotný soud mnohdy v navazující judikatuře odkazuje, bylo vydáno v nálezu Pl. ÚS 24/10 ze dne 22. března 2011. V tomto rozhodnutí dospěl Ústavní soud mimo jiné k tomuto závěru: *„Vedle tradičního vymezení soukromí v jeho prostorové dimenzi (ochrana 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.“*[100] Tímto rozhodnutím se tedy Ústavní soud snaží o vymezení minimálně tří podsložek soukromí, a to a) ochrana soukromí, b) sociální sebeurčení a c) svoboda rozhodování o sobě samém. Za zmínku dále stojí, že Ústavní soud rozlišuje mezi aktivní a pasivní složkou soukromého života, když uvádí: *„Jinými slovy, právo na respekt k soukromému životu zahrnuje garanci sebeurčení ve smyslu zásadního rozhodování o sobě samém, včetně rozhodování o uspořádání vlastního života, což lze označit jako aktivní seberealizační komponent*

[98] Jde o zkratku tzv. „Social security number“, což je jakousi obdobou našeho rodného čísla.
[99] Solove, D. J., Schwartz, P. M. *Privacy Law Fundamentals*, Portsmouth: International Association of Privacy Professionals, 2017, s. IX.
[100] Nález Ústavního soudu ČR ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10.

osobního sebeurčení. Za pasivní oblast soukromého života můžeme označit tu osobnostní sféru, která je imanentní samotnému lidství, jako je především lidská důstojnost, osobní čest, dobré jméno a také vnitřní potřeba sociálního kontaktu a sociálního začlenění. Soukromý život tak obsáhne nejen internum, nýbrž i externum, které se vztahuje k obchodním, pracovním nebo i sociálním aktivitám."[101] Dále je možné identifikovat celou řadu navazujících rozhodnutí Ústavního soudu ČR.[102]

Rozhodnutí jiných soudů se obvykle zaměřují již na specifické otázky ochrany soukromí a vybraným případům z těchto rozhodnutí je věnována pozornost dále v této práci. Na tomto místě se však nabízí pojednat o judikatuře ESLP. Na úvod snad lze jen pro úplnost poznamenat, že to byl právě ESLP, který dovodil, že nelze podat jednoznačnou definici soukromí a je vždy nutné ho vykládat podle konkrétních skutkových okolností.[103] Možná i z toho důvodu je příslušná judikatura velmi kazuistická. ESLP tak například dovozuje, že stát nemá jen povinnost zdržet se nadměrných zásahů do soukromí osob, ale má též zabezpečit opatření k respektu soukromého života jednotlivců.[104] Pokud má soud zasahovat do soukromí jedince, musí existovat jasné mantinely, aby se jedinec mohl proti takovým zásahům bránit.[105] Ještě zajímavější a pro tuto práci významnější může být princip rozumného očekávání soukromí (*reasonable expectation of privacy*) subjektů. Tento koncept byl například vyjádřen při posuzování toho, zda je zaměstnavatel oprávněn narušovat soukromí zaměstnance na pracovišti tím, že odposlouchává jeho hovory, aniž by o tom zaměstnance předem informoval.[106] Svůj význam má též ze strany ESLP zavedený test porušení čl. 8, kdy je pomocí určitých otázek zkoumáno, zda došlo k zásahu do práva na ochranu soukromí či nikoliv.[107] Pokud jde o jednotlivé podsložky práva na ochranu soukromí, lze v judikatuře ESLP vysledovat několik sfér soukromí, kterým se ESLP

---

[101] Nález Ústavního soudu ČR ze dne 6. března 2012, sp. zn. Pl. ÚS 1586/09.
[102] Například nález Ústavního soudu ČR ze dne 1. března 2000, sp. zn. II. ÚS 517/99, či nález Ústavního soudu ČR ze dne 7. dubna 2010, sp. zn. I. ÚS 22/10.
[103] Uvedené bylo dovozeno především v rozhodnutí ESLP ze dne 16. září 2008, ve věci Pay v. Spojené království, č. stížnosti 32792/05 (srov. Harris, D. J., O'boyle M. a kol. *Law of the European Convention on Human Rights.* Third edition. Oxford, United Kingdom: Oxford University Press, 2014, s. 364).
[104] Rozhodnutí ESLP ze dne 7. července 1989 ve věci Gaskin v. Spojené království, č. stížnosti 10454/83.
[105] Rozhodnutí ESLP ze dne 4. května 2000 ve věci Rotaru v. Rumunsko, č. stížnosti 28341/95.
[106] Blíže viz podkapitola 3.3.
[107] V rámci tohoto testu dochází ke zkoumání následujících otázek: Došlo k porušení práva? Je omezení práva v souladu se zákonem? Má omezení práva legitimní cíl? Jde o omezení nezbytné v demokratické společnosti? Srov. Fialová, E. *Ochrana soukromí ve světle judikatury Evropského soudu pro lidská práva*. Časopis pro právní vědu a praxi. 2012, roč. 20, č. 2, s. 122.

pravidelně ve své judikatuře věnuje. Jedná se o ochranu rodinného života, práva na život v dobrém životním prostředí, ochranu obydlí, korespondence, sexuality a osobních údajů.[108]

Obdobně má ve vztahu k výkladu práva na ochranu soukromí význam též judikatura Soudního dvora Evropské unie (dále jen „SDEU"), jelikož Evropská unie už dávno není pouhou hospodářskou integrací, ale proniká i do jiných oblastí, včetně ochrany lidských práv. Jejich ochrana byla do práva Evropské unie závazně zakotvena sice až spolu s přijetím LZPEU v roce 2009, avšak SDEU, resp. jeho předchůdce, kterým byl Evropský soudní dvůr, se vybraným základním právům věnoval již mnohem dříve.[109] Nejinak tomu bylo u práva na ochranu soukromí. V souvislosti s předmětem této práce stojí za zmínku zejména rozhodnutí SDEU ze dne 20. května 2003 ve spojených věcech C-465/00, C-38/01 a C-139/01. V tomto rozhodnutí se SDEU zabýval výkladem Směrnice a možnostmi předání platů zaměstnanců určitých veřejných subjektů ke kontrole, což v konečném důsledku znamenalo zpřístupnění informací o platech těchto osob široké veřejnosti. Soud se přitom při výkladu Směrnice a používaného pojmu ochrany soukromí neváhá opřít o čl. 8 EÚLP. Zdůraznil přitom, že *„ačkoliv pouhé zaznamenání osobních údajů týkajících se příjmů vyplacených zaměstnavatelem svým zaměstnancům nemůže jako takové představovat zásah do soukromí, sdělení těchto údajů třetí osobě, v tomto případě veřejnému orgánu, porušuje ochranu soukromí dotyčných osob"*.[110] Přesto však rovněž dovodil, že žádný článek Směrnice (potažmo čl. 8 EÚLP) *„nebrání takové vnitrostátní právní úpravě, jakou je úprava dotčená ve věcech v původních řízeních, za předpokladu, že je prokázáno, že široké zveřejnění […] je nezbytné a vhodné ve vztahu k cíli řádné správy veřejných prostředků sledovanému ústavodárcem […]".*[111] V této souvislosti se pouze nabízí otázka, nakolik je takové zveřejnění v dnešní době nezbytné a zda nemůže být stejného účelu dosaženo pouze zpřístupněním stanovených údajů orgánu dohledu.

---

[108] Fialová, E. *Ochrana soukromí ve světle judikatury Evropského soudu pro lidská práva*. Časopis pro právní vědu a praxi. 2012, roč. 20, č. 2, s. 124-125.

[109] Za první uznání práva na ochranu soukromí bývá považováno rozhodnutí ve věci *Stauder v. Město Ulm* z roku 1969, ve kterém se soud přihlašuje k ochraně základních lidských práv, která jsou obsažena v obecných principech práva ES (srov. Pomahač, R., Pítrová, L. *Průvodce judikaturou Evropského soudního dvora*. Díl 1. Praha: Linde, 2000, s. 88-89).

[110] Rozhodnutí SDEU ze dne 20. května 2003 ve spojených věcech C-465/00, C-38/01 a C-139/01, bod 74.

[111] Tamtéž (výrok rozhodnutí).

2.3 Úvodní poznámky k ochraně osobních údajů

Oproti ochraně soukromí je ochrana osobních údajů teprve doslova v plenkách a nemůže se pochlubit stejně dlouhou historií své existence. Na druhou stranu skýtá mnohem větší penzum specifických pravidel. Záměrem této podkapitoly je nabídnout stručný a obecný úvod a historický pohled na problematiku ochrany osobních údajů v České republice a osvětlit způsoby ochrany před neoprávněným zpracováním osobních údajů. Následně to poslouží k výkladu v další podkapitole srovnávající ochranu osobních údajů s ochranou osobnosti.

2.3.1 Historie ochrany osobních údajů

Předmětem ochrany osobních údajů je naplnění a bližší úprava práva na ochranu soukromí vyplývajícího právě ze situací, kdy dochází ke zpracování osobních údajů (blíže jsou tyto pojmy a působnosti ochrany osobních údajů vysvětleny a zkoumány v podkapitole 6.1). Vazba na ochranu soukromí byla patrná i z ustanovení § 1 ZOOÚ, které definovalo předmět úpravy ZOOÚ a v rámci kterého se uvádělo: *„Tento zákon […] k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.“*[112] Na druhou stranu byla ochrana osobních údajů od ochrany soukromí částečně oddělena a žije si svým vlastním životem. O tom svědčí existence specifických regulací jako Směrnice, GDPR, ale dokonce též závazných pravidel vyšší právní síly, zejména čl. 8 LZPEU, případně též čl. 16 odst. 1 SFEU a Úmluvy 108.

Právě s Úmluvou 108, přijatou na půdě Rady Evropy, bývá spojován vznik ochrany osobních údajů jako samostatného odvětví. Ten se tedy traduje od počátku 80. let 20. století. V České republice se první norma věnující se ochraně osobních údajů objevila ještě přibližně o deset let poté a šlo o zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Z názvu je však patrné, že nešlo o obecně platný předpis (ve smyslu, že by se uplatnil na veškeré zpracování osobních údajů), ale týkal se omezeně jen informačních systémů.[113] Proto byly významnější až přípravy implementací Směrnice v souvislosti s přípravou vstupu České republiky do Evropské unie, které probíhaly již na konci 90. let

[112] Podobně též § 1 ZZOÚ.
[113] Ten byl v § 4 citovaného zákona definován jako „*funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Každý informační systém zahrnuje informační základnu, technické a programové prostředky, technologie a procedury a pracovníky.*“.

20. století. Výsledkem tohoto procesu bylo následně v roce 2000 přijetí ZOOÚ jakožto prvního obecného předpisu věnujícího se této problematice. [114]

ZOOÚ byl účinný téměř 20 let, než došlo k jeho nahrazení ze strany nařízení GDPR. Uplatňování pravidel stanovených tímto předpisem mělo přitom postupně rostoucí tendenci, a to zejména v souvislosti s tím, jak docházelo k rozšiřování informačních technologií a možností sdílení a přenosu informací. Ani přesto však nebylo povědomí o této právní regulaci příliš rozšířené. Dodržování souladu bylo zajišťováno spíše ze strany společností majících široké portfolio zákazníků (banky, operátoři, registry či společnosti působící v prostředí internetu), a to mnohdy spíše s ohledem na bezpečnostní rizika. Informační povinnosti, resp. příslušná práva obvykle naplňována nebyla. Jedním z důvodu mohlo být relativně nižší rozšíření povědomí o této regulaci a dále to mohlo souviset též se spíše nižšími horními hranicemi pokut, které hrozily za porušení stanovených pravidel.[115] V rámci rozhodování, zda docílit plného souladu s těmito pravidly, což obnášelo revidovat interní procesy a systémy a vynaložit vysoké náklady, nebo riskovat riziko udělení sankce za porušení pravidel, obvykle vyhrávala druhá varianta.

Nařízení GDPR bylo přijato mimo jiné s ohledem na tato negativa. Kromě zavedení vysokých hranic pro pokuty za porušení pravidel[116] bylo nepochybně cílem tohoto nařízení dosažení obecně vyššího souladu s příslušnými pravidly a rozšíření povědomí o této regulaci mezi širokou veřejnost. V posledních dvou letech, kdy probíhaly přípravy na příchod nařízení, se toho do určité míry podařilo dosáhnout. Nakolik to však bude s trvalým efektem, bude možné hodnotit až s odstupem času.

2.3.2 Ochrana před neoprávněným zpracováním osobních údajů

Pokud jde o způsoby ochrany před neoprávněným zpracováním osobních údajů z hlediska konkrétního jedince (subjektu údajů), nabízí se několik variant. Jedním ze základních způsobů je ochrana „svépomocí“, spočívající v tom, že si jedinec vyžádá veškeré údaje, které o něm správce (např. zaměstnavatel) zpracovává. Ten je povinen mu ve stanovené lhůtě vyhovět a vydat mu nejen kopie jeho osobních údajů, ale také další související informace o zpracování jeho osobních údajů.[117] V návaznosti na to samozřejmě

[114] Kučerová, A. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. VI.
[115] Maximální možná sankce za porušení pravidel podle ZOOÚ činila v případě právnických osob a podnikajících fyzických osob 10 000 000 Kč (§ 45 ZOOÚ).
[116] Až do výše 20 000 000 eur, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší (srov. čl. 83 GDPR).
[117] A to na základě čl. 15 GDPR.

mohou připadat do úvahy další práva, kterými jsou zejména právo na opravu osobních údajů, právo na výmaz osobních údajů, právo odvolat souhlas se zpracováním osobních údajů či právo vznést námitku.[118]

S ohledem na zapojení třetí osoby do sporu mezi jedincem (subjektem údajů) a správcem je již o poznání významnějším právem právo podat stížnosti dozorovému orgánu, tj. ÚOOÚ, dle čl. 77 GDPR. V důsledku podání stížnosti může dojít k celé řadě následků v případě, že dojde ke zjištění, že pravidla na ochranu osobních údajů byla ve vztahu k příslušnému jedinci (či obecně) porušena. Pravomoc dozorového orgánu k tomuto je svěřena v rámci čl. 58 GDPR, přičemž kromě již zmiňovaného udělení správní pokuty může dozorový orgán rovněž udělit napomenutí, uložit dočasné nebo trvalé omezení zpracování, nařídit opravu či výmaz osobních údajů, odebrat osvědčení dle čl. 42 GDPR apod.

Kromě výše uvedeného není dále vyloučeno domáhat se svých práv přímo u soudu, a to s odkazem na čl. 79 odst. 1 GDPR, který uvádí: *„Aniž je dotčena jakákoli dostupná správní či mimosoudní ochrana, včetně práva na podání stížnosti u dozorového úřadu podle článku 77, má každý subjekt údajů právo na účinnou soudní ochranu, pokud má za to, že jeho práva podle tohoto nařízení byla porušena v důsledku zpracování jeho osobních údajů v rozporu s tímto nařízením.“* Poškozený subjekt údajů se tedy může svých práv podle GDPR domáhat sám před soudem. Toto bude proveditelné zejména u práv, resp. povinností, kdy je správcům osobních údajů stanovena nějaká konkrétní povinnost ve vztahu k subjektům údajů. Půjde především o práva přiznaná dle čl. 15 až 22 nařízení GDPR. Může se ale také jednat o domáhání se náhrady způsobené újmy (podle čl. 82 GDPR). Tato možnost je jistě chvályhodná, i když na druhou stranu nelze očekávat, že bude v praxi příliš využívaná, jelikož takové soudní řízení je zatíženo náklady (obvykle nikoliv malými), kdežto podání stížnosti ÚOOÚ dle již zmiňovaného čl. 77 GDPR má do velké míry podobný efekt, ale v podstatě žádnými náklady zatíženo není.[119]

2.4 Vztah ochrany osobnosti a osobních údajů

Ochrana osobnosti upravená v ObčZ se s ochranou osobních údajů obsaženou v nařízení GDPR, potažmo v ZZOÚ, příliš nepotkává. To platí zejména, pokud jde o terminologii a principy ochrany osobních údajů zakotvené v nařízení GDPR. Důvodem je

[118] Blíže srov. výklad v podkapitole 7.2.
[119] Obdobně tomu bylo ostatně za platnosti ZOOÚ, kdy podobnou možnost upravoval § 21 ZOOÚ.

především skutečnost, že ochrana osobnosti vychází ze soukromého práva, kdežto ochrana osobních údajů má veřejnoprávní charakter. Úprava ochrany osobnosti v ObčZ se samozřejmě věnuje kromě otázek nedotknutelnosti člověka, ochrany života a fyzické integrity též ochraně soukromí a ochraně projevů osobní povahy. A právě tato část má k ochraně osobních údajů nepochybně nejblíže. V níže uvedeném textu je pojednáno nejprve o podobných prvcích těchto právních oblastí, zda představují shodné či odlišné množiny, následně o jejich (dalších) odlišnostech a nakonec je nabídnuto shrnutí obsahující zamyšlení nad budoucí podobou právních norem ochrany soukromí a popis další systematiky této práce.

2.4.1 Podobné, nikoliv však stejné množiny

Blízkost ochrany soukromí a ochrany osobních údajů deklaruje samo nařízení GDPR, v jehož preambuli se lze dočíst, že *„nařízení ctí všechna základní práva a dodržuje svobody a zásady uznávané Listinou, jak jsou zakotveny ve Smlouvách, zejména respektování soukromého a rodinného života, obydlí a komunikace, ochranu osobních údajů […]“.*[120] Podobně je též v ZZOÚ vyjádřeno: *„Tento zákon […] k naplnění práva každého na ochranu soukromí upravuje práva a povinnosti při zpracování osobních údajů.“*[121] Podobnost pak lze identifikovat i v obsahu, resp. v chráněných statcích.

To potvrzuje také teorie, která ochranu osobních údajů za součást ochrany jednoznačně považuje.[122] Nonnemann v této souvislosti dále dovozuje, že mezi ochranou osobnosti a osobních údajů platí vztah obecné a zvláštní úpravy, přičemž se zabývá otázkou rozlišování toho, kdy se má postupovat podle soukromoprávního a kdy podle veřejnoprávního předpisu.[123] Ač je úvaha o obecné a zvláštní úpravě chvályhodná, jelikož by tento závěr znamenal teoretické sblížení obou úprav, autor této práce se s tímto závěrem neztotožňuje a považuje obě úpravy za paralelní, na sobě nezávislé (právě z důvodu svého soukromoprávního či veřejnoprávního charakteru), byť obsahem a chráněnými statky částečně se překrývající. Důležité jsou totiž zejména odlišné důsledky za nedodržování

[120] Srov. preambule (4) nařízení GDPR.
[121] Srov. § 1 ZZOÚ.
[122] Knap, K., Švestka, J., Jehlička, O., Pavlík, P., Plecitý, V. *Ochrana osobnosti podle občanského práva*. 4., podstatně přeprac. a dopl. vyd. Praha: Linde, 2004. s. 395.
[123] Nonnemann, F. *Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů*. Právní rozhledy. 2012, 20(13), s. 507-508.

stanovených povinností.[124] Rovněž platí, že obvykle bude namístě aplikovat obě právní úpravy naráz.[125]

Je dokonce možné dovodit, že jedna oblast je podmnožinou druhé? Či naopak? Je zřejmé, že kdykoliv dojde k porušení ochrany osobnosti, nebude se vždy jednat o porušení ochrany osobních údajů. Ochrana osobnosti je širší množinou chránící o mnoho více aspektů života jedinců. Nabízí se pak otázka, zda porušení pravidel o ochraně osobních údajů bude vždy porušením ochrany osobnosti? Nikoliv. Nejde o lehkou otázku, nicméně je obecně zřejmé, že regulace ochrany osobních údajů nemusí mít vždy přímý dopad na jedince. Jakým způsobem bude například porušena ochrana osobnosti jedince, pokud správce osobních údajů nepovede záznamy o činnostech zpracování ve smyslu čl. 30 GDPR? Dle autora této práce nijak, jde o povinnost, která nemá přímý dopad na jedince.

Existuje však mnoho povinností, u kterých bude porušení ochrany osobnosti zřejmé, pokud například bude docházet ke zpracování osobních údajů bez odpovídající právního základu. Například správce neoprávněně zveřejní osobní údaje. Pak je bezpochyby, že k porušení ochrany osobnosti (a soukromí) došlo. Vedle toho je ale v nařízení GDPR upravena i řada povinností, u kterých nebude odpověď tak zřejmá. Bude porušením ochrany osobnosti, pokud nebude splněna informační povinnost podle čl. 13 GDPR? Tato povinnost má nepochybně vztah k jedinci, ale může jejím nesplněním dojít k porušení osobnosti jedince? Odpověď nebude snadná a bude záležet na konkrétních skutkových okolnostech, především v čem spočívalo nesplnění informační povinnosti, jaké to mělo důsledky pro jedince apod. Další rozbor této otázky přesahuje rozsah a předmět této práce. Cílem však bylo poukázat na skutečnost, že obě právní oblasti jsou odlišnými množinami, které se v určitých aspektech mohou překrývat a v určitých se překrývat nebudou. Bude vždy ad hoc záležet na tom, do jaké míry došlo k zásahu do osobnosti člověka.

Toto je v zásadě i v souladu s názorem ÚOOÚ, který se snaží obě oblasti sbližovat, když uvádí, že *„každé zpracování osobních údajů představuje zásah do soukromí jednotlivce. Aby tento zásah a celé zpracování bylo legální, je třeba, aby správce ve všech případech, kdy je to možné, posoudil případné způsoby zpracování a zvolil ten, který do soukromí subjektů údajů zasáhne v nejmenší míře. V opačném případě nebude zpracování*

[124] Tomu přispívá i skutečnost, že (česká) soudní rozhodnutí se zatím obvykle věnují výhradně ochraně osobnosti a prakticky nikdy se nezaobírají ochranou osobních údajů. Příkladem může být například rozhodnutí ve věci Kasalova Pila (rozhodnutí Nejvyššího soudu ČR ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011). Byť i v této rovině se již rozdíly částečně stírají, srov. ustanovení čl. 79 odst. 1 nařízení GDPR.
[125] Tuto možnost samozřejmě Nonnemann také nevylučuje (op. cit. sub. 123).

v souladu se zákonem o ochraně osobních údajů a správce se vystavuje riziku kontroly a uplatnění opatření k nápravě ze strany Úřadu s tím, že toto opatření může v krajním případě představovat i zákaz celého prováděného zpracování osobních údajů.".[126] Na druhou stranu však ÚOOÚ zároveň jasně uvádí, že ochrana osobních údajů se aplikuje až v situaci, kdy někdo provádí systematicky určitou operaci nebo soustavu operací s osobními údaji, a že se jedná o provedení čl. 10 odst. 3 LZPAS, na rozdíl od ochrany soukromí, která je provedením čl. 10 odst. 2 LZPAS.

2.4.2 Další odlišnosti

Základní odlišností je, že ochrana osobních údajů se má primárně vztahovat, zjednodušeně řečeno, na soustavné operace zpracování.[127] V tomto ohledu je důležitý článek 2 nařízení GDPR, který upravuje věcnou působnost tohoto předpisu a který omezuje jeho aplikaci jen *„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".* Důsledkem tohoto ustanovení a z podstaty pojmu „zpracování" osobních údajů vyplývá, že ochrana osobních údajů se neuplatní na nahodilé operace s osobními údaji.[128] Nic však neomezuje, aby se na tyto případy plně uplatnila ochrana osobnosti. Ochrana osobnosti se naopak může plně uplatnit i na případy nikoliv nahodilé operace zpracování osobních údajů, které jsou plně v režimu nařízení GDPR.[129]

Za rozbor dále stojí míra detailu či rozsah obou právních úprav. Ochrana soukromí podaná v ObčZ si vystačí s poměrně málo ustanoveními upravujícími ochranu podoby a soukromí (obsaženou v § 84 až 90 ObčZ) a definováním obecných principů (jako je např. v § 19 odst. 2 ObčZ uvedená nezcizitelnost přirozených práv, kterým je i právo na

---

[126] Srov. stanovisko ÚOOÚ č. 6/2009: *Ochrana soukromí při zpracování osobních údajů*. Listopad 2009, aktualizace únor 2014.
[127] K pojmu zpracování srov. bod 6.1.2.
[128] Shodně Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 66.
[129] Odlišně Nonnemann, který uvádí, že bavíme-li se o ochraně podoby člověka dle ObčZ, bude příslušná občanskoprávní úprava *„omezena pouze na nahodilé či jednorázové pořízení či zpřístupnění nebo zveřejnění podoby člověka nebo na zpracování osobních údajů, které bude provádět fyzická osoba výlučně pro svoji potřebu, či na nahodilé, neúmyslné, shromažďování osobních údajů"*. Obdobný závěr Nonnemann též dovozuje ve vztahu k pořizování obrazových a zvukových záznamů, kde dokonce uvádí, že *„z tohoto důvodu lze dle mého názoru konstatovat, že ne nepodstatná část úpravy ochrany osobnosti v této části nového zákoníku je obsoletní"* (srov. Nonnemann, F. *Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů*. Právní rozhledy. 2012, 20(13), s. 507-508).

ochranu soukromí).[130] Naopak ochrana osobních údajů je relativně podrobnou právní úpravou, jejíž základ je upraven v nařízení GDPR, ZZOÚ a v celé řadě dalších právních předpisů. Důsledky tohoto rozdílu lze pozorovat například na situaci nesvobodného zásahu do ochrany osobnosti či osobních údajů, který by snad měl být zhojen „souhlasem" subjektu. Zatímco v rámci ObčZ se bude při domáhání právní ochrany možné opírat pouze o obecnou nezcizitelnost přirozených práv, v nařízení GDPR bude možné jasně poukázat na neexistenci svobodného souhlasu (čl. 4 odst. 11), porušení podmínek vyjádření souhlasu (čl. 7), na porušení zákonnosti zpracování (čl. 6) i na porušení zásad zpracování (čl. 5).

2.4.3 Shrnutí

Výše uvedené jen podtrhuje skutečnost, že právní úprava ochrany osobnosti a soukromí a právní úprava ochrany osobnosti jsou relativně samostatné fenomény, ač jsou si předmětem chráněného statku velmi blízké. Do budoucna by jistě stálo za to, aby došlo k jejich většímu sblížení, a to alespoň explicitním zahrnutím ochrany osobních údajů v rámci ObčZ pod ochranu podoby a soukromí (§ 84 a násl.).[131] Že je ochrana osobních údajů součástí ochrany soukromí, už přitom dlouhou dobu potvrzuje judikatura ESLP i již dlouhou dobu platná a závazná LZPEU. Přesto tuto skutečnost český zákonodárce nevzal více v potaz při přípravě (nového) ObčZ. Ustanovení, která by měla být podle názoru autora této práce zahrnuta do ObčZ, by přitom nemusela být nikterak podrobná, ale došlo by tím alespoň k jasnému vymezení vztahu těchto právních oblastí. V rámci občanského zákoníku by došlo též k vyjasnění vztahu ochrany osobních údajů a jiných blízkých chráněných statků, kterými je ochrana podoby, písemností osobní povahy nebo zvukového či obrazového záznamu, k ujasnění režimu určování právního základu a režimu souhlasů se zpracováním osobních údajů či zásahů do ochrany soukromí.

Na druhou stranu je zřejmé, že regulace ochrany osobních údajů v rámci nařízení GDPR je spíše veřejnoprávní úpravou a ochrana osobnosti v občanském zákoníku je ryze soukromoprávní, a proto tyto dvě oblasti nelze jednoduše směšovat. Rozdílné jsou povinnosti, které musí adresáti norem dodržovat, rozdílný je jejich rozsah a podoba, rozdílné jsou prostředky ochrany proti porušení stanovených povinností. Ze všech těchto důvodů je

---

[130] Kromě toho jsou vybraná ustanovení na ochranu osobnosti a soukromí obsažena též ve zvláštních předpisech. Příkladem nechť je ustanovení § 316 odst. 2 ZPr omezující možnost zaměstnavatele narušovat soukromí zaměstnance. O tomto ustanovení je dále detailně pojednáno v podkapitole 5.4.

[131] V případě existence takové legislativní vazby by efektivně došlo k odstranění problému, že ochrana osobních údajů má spíše veřejnoprávní charakter. V podstatě by následně byla ochrana soukromí s veřejnoprávní regulací, obdobně jako je tomu obecně v případě pracovního práva.

v této práci následně zvlášť pojednáno o ochraně osobnosti v pracovním právu a dále samostatně o ochraně osobních údajů zaměstnanců. Byť porušení jednoho může mnohdy znamenat i porušení druhého, nemusí tomu tak být vždy, jak bylo vysvětleno výše v tomto bodě. Bohužel, ještě o něco složitější je situace v rámci pracovněprávních vztahů, kde je ochrana osobnosti a soukromí posilována ve prospěch slabší strany, zaměstnance, a charakter norem je proto mnohdy smíšený či ryze veřejnoprávní a také prostředky ochrany jsou mnohdy veřejnoprávní. Přesto jde o jinou oblast, na kterou dohlížejí jiné orgány. Proto i z hlediska lepší systematiky je o ochraně osobnosti a osobních údajů následně pojednáno samostatně ve zvláštních kapitolách s tím, že je poukazováno na vzájemné vazby a podobnosti.

II. ČÁST OCHRANA OSOBNOSTI

3 Úvodní východiska ochrany osobnosti v pracovním právu

Ochrana osobnosti na pracovišti, resp. v rámci úpravy norem pracovního práva, není totožná s obecnou úpravou ochrany osobnosti, jak o ní bylo pojednáno výše. Nelze totiž říci, že by bylo možné shodně nahlížet na zaměstnance a zaměstnavatele, například na spotřebitele a na podnikatele nebo na jakýkoliv obecný vztah dvou občanů. Jouza v té souvislosti uvádí, že „v *pracovněprávních vztazích má ochrana osobnosti člověka širší význam*“.[132] Toto je dáno specifičností vztahu mezi zaměstnancem a zaměstnavatelem a dále charakterem právních norem pracovního práva. Proto jsou v této kapitole tato specifika blíže rozebrána jako klíčové prvky pro správné chápání ochrany osobnosti na pracovišti. Obsahem této kapitoly je především analýza základních východisek ochrany osobnosti a soukromí zaměstnanců v oblasti pracovního práva, a to včetně analýzy související judikatury, zejména zahraniční. Jsou zejména popsány základní principy vztahů zaměstnance a zaměstnavatele, charakter norem pracovního práva a koncept legitimního očekávání soukromí na pracovišti.

3.1 Vztah zaměstnance a zaměstnavatele

Vztah mezi zaměstnancem a zaměstnavatelem je ve své podstatě ryze ekonomický. Zaměstnavatel v tomto vztahu požaduje po zaměstnanci plnění určitých úkolů a nabízí mu za to odměnu, zaměstnanec za tuto odměnu poskytuje zaměstnavateli své schopnosti a svou pracovní sílu. Jde tak v podstatě o ekonomickou transakci.[133] V tradičním pojetí tak zaměstnavatel činí, aby dosáhl udržení či rozvoje svého podnikání. Naopak zaměstnanec požadované úkoly plní obvykle jen proto, aby byl schopen si zajistit prostředky pro svou obživu. Zaměstnanec se tak může dostávat a mnohdy také dostává do značné závislosti na zaměstnavateli, resp. jím vyplacené mzdě či jiné odměně. Právě proto je ochraně zaměstnanců věnována značná legislativní pozornost. To platí pro kontinentální právní systém, především země Evropské unie. Naopak v rámci Spojených států amerických je

---

[132] Jouza, L. *Ochrana osobnosti zaměstnance v pracovněprávních vztazích*. Bulletin advokacie. 2014, č. 6, s. 26.

[133] Block, R. N., Berg, P., Belman, D. *The Economic Dimension of the Employment Relationship*. In *The Employment Relationship: Examining Psychological and Contextual Perspectives* [online]. Oxford: Oxford University Press, 2004, s. 94. [cit. 2019-01-05]. Dostupné z: https://msu.edu/~block/documents/Coyle-ch05RBChangesJan2304.pdf

volen poněkud volnější model volného trhu, založený na individualismu, ve kterém chybí bližší regulace pracovních smluv.[134]

Ve smyslu platného práva jsou zaměstnanec i zaměstnavatel definováni ve vztahu k výkonu závislé práce. Zaměstnavatel jako ten, pro koho má být vykonávána závislá práce, a zaměstnanec jako ten, kdo ji má vykonávat. Důležité je rovněž zmínit, že zaměstnanec musí být vždy fyzickou osobou, a proto bude v tomto vztahu vždy relevantní zkoumat ochranu osobnosti zaměstnance tak, jak je chápána v této práci.[135] Základní charakteristikou vztahu zaměstnavatele a zaměstnance je tedy výkon závislé práce zaměstnance pro zaměstnavatele. Na rozdíl od common law tak v našem právním prostředí obvykle nepanují pochybnosti o tom, kde je a kdo není zaměstnanec.[136] Je totiž jasně stanoveno, že závislá práce může být vykonávána výlučně v základním pracovněprávním vztahu, kterými jsou pracovní poměr a právní vztahy založené dohodami o pracích konaných mimo pracovní poměr (nestanoví-li zvláštní předpisy jinak).[137]

Pokud jde o obsah závislé práce, je v rámci ustanovení § 2 odst. 1 ZPr uvedeno, že „*závislou prací je práce, která je vykonávána ve vztahu nadřízenosti zaměstnavatele a podřízenosti zaměstnance, jménem zaměstnavatele, podle pokynů zaměstnavatele a zaměstnanec ji pro zaměstnavatele vykonává osobně*“. Tím je tedy jasně reflektována nevyváženost tohoto vztahu vyplývající z jeho ekonomické podstaty. Důsledkem této skutečnosti pak je, že v rámci pracovního práva dochází k značnému omezení smluvní volnosti, a to ve prospěch zaměstnance. Je dokonce možné konstatovat, že z tohoto principu vychází celé pracovní právo, kdy jeho smyslem je v první řadě chránit slabší stranu, tj. zaměstnance. Ochrana zaměstnance jakožto subjektu, který je v daném vztahu obvykle ve slabším postavení, se však neomezuje jen na limitaci možností kontraktace. Pracovní právo chrání zaměstnance v celé řadě dalších oblastí, například při definování podmínek

---

[134] Tamtéž, s. 100. I přesto je možné konstatovat, že Spojené státy americké mají velmi kvalitní antidiskriminační zákonodárství, které podstatně omezuje smluvní svobodu stran při uzavírání pracovních smluv (srov. Bělina, M. a kol. *Pracovní právo.* 7. doplněné a podstatně přepracované vydání 2017. Praha: C. H. Beck, 2017, s. 4-8).

[135] Není sporu o tom, že i právnické osoby mají právo na ochranu soukromí, to se však omezuje na určité složky, jako je například ochrana názvu právnické osoby, ochrana pověsti, ochrana obchodního tajemství apod. Ve většině jde tedy o jiné složky ochrany osobnosti a soukromí, než jak jsou chápány v této práci.

[136] V rámci *common law* se vztah mezi zaměstnancem a zaměstnavatelem obvykle zkoumá podle právních testů kontroly druhou osobou, finanční závislostí a existencí právní konstrukce vzájemného vztahu, přičemž jejich posouzení závisí na faktických okolnostech vztahu mezi dvěma osobami (srov. např. ROGERS, Brishen. *Employment Rights in the Platform Economy: Getting Back to Basics* [online]. Harvard Law & Policy Review, vol. 10, 2016, s. 484. [cit. 2019-02-01]. Dostupné z: https://harvardlpr.com/wp-content/uploads/sites/20/2016/06/10.2_7_Rogers.pdf)

[137] Srov. ustanovení § 3 Zpr.

bezpečnosti práce nebo informační povinnosti zaměstnavatele, v oblasti kolektivního vyjednávání, ale i z hlediska ochrany soukromí zaměstnance při výkonu závislé práce (i mimo ni), což je klíčové z hlediska zaměření této práce.

V souvislosti s výše zmíněným pojmem slabší strana se nabízí zamyšlení nad průnikem pracovněprávních vztahů a občanskoprávní legislativy. Základní premisa tohoto vztahu je dnes již jednoznačně vymezena v ustanovení § 4 ZPr, podle kterého se ObčZ se na pracovně právní vztahy použije vždy, nemá-li ZPr svou vlastní úpravu, a to v souladu se základními zásadami pracovněprávních vztahů.[138] Jedná se o princip subsidiarity, který se do právního řádu dostal v návaznosti na zásah Ústavního soudu ČR.[139] Samozřejmostí je tak použití obecné úpravy týkající se osobnosti a svéprávnosti, zastupování, právních jednání, právních událostí apod. na pracovní vztahy. Určité instituty se uplatní jen v určitých mezích, ať už s odkazem na zásady pracovního práva (odstoupení od smlouvy, započtení apod.), nebo s odkazem na jejich explicitní omezení (např. smluvní pokuta). V určitých případech je pak dokonce stanoven explicitní zákaz.[140]

Z pohledu vztahu zaměstnance a zaměstnavatele jsou zajímavá ustanovení ObčZ, která mají za cíl chránit slabší stranu. Ta je v ObčZ definována jako osoba, která vůči podnikateli v hospodářském styku vystupuje mimo souvislost s vlastním podnikáním.[141] Jedná se však o vyvratitelnou domněnku a Hůrka například dovozuje, že zaměstnance *„nelze považovat za slabší stranu automaticky, můžeme nalézt vztahy, kdy zaměstnanec má silné postavení na trhu práce, je finančně zajištěn a jeho závislost na existenci daného právního vztahu není vysoká“.*[142] Bez ohledu na tento závěr se tato domněnka obvykle u zaměstnance uplatní. Tento závěr může být relevantní též hlediska ochrany osobnosti zaměstnance. Vyjdeme-li totiž ze skutečnosti, že ObčZ upravuje ochranu slabší strany při uzavírání smluv adhézním způsobem ve smyslu § 1798 ObčZ a násl., uplatní se na zaměstnance též ochrana před nečitelnými, nesrozumitelnými či zvlášť nevýhodnými doložkami.[143] Zejména pak nesrozumitelnost může být v této souvislosti relevantní a za určitých okolností by se zaměstnanec mohl dovolávat například nesplnění povinnosti informovat zaměstnance o prostředcích kontroly ve smyslu § 316 ZPr (ač by se takovéto

[138] Srov. § 4 ZPr.
[139] Nález Ústavního soudu ČR ze dne 12. března 2008, sp. zn. Pl. ÚS 83/06, vyhlášený pod č.116/2008 Sb.
[140] Srov. § 346d ZPr.
[141] Srov. § 433 odst. 2 ObčZ.
[142] Srov. Hůrka, P. *Změny v pracovním právu v souvislosti s novým občanským zákoníkem*. Právní rozhledy. 2014, 22(7), s. 236.
[143] Srov. § 1800 ObčZ.

neplatnosti dalo patrně dovolávat i s odkazem na zdánlivost právního jednání dle § 553 ObčZ, ustanovení o adhezních smlouvách jsou oproti nim výhodnější s ohledem na přenos důkazního břemene).

Závěrem lze tak jen shrnout, že nevyrovnanost vztahu zaměstnance a zaměstnavatele je klíčovým prvkem existence pracovního práva a právní ochrany zaměstnance, která je navíc dále podpořena i ochranou zakotvenou v rámci ObčZ. Jak bude poukázáno dále, toto má zcela klíčový vliv na obsah a rozsah ochrany osobnosti a osobních údajů zaměstnance na pracovišti.

3.2 Charakter právních norem pracovního práva

Z hlediska předmětu této práce není významná jen specifičnost vztahu zaměstnance a zaměstnavatele, která byla popsána výše. Vedle toho to jsou rovněž další veřejnoprávní prvky v individuálním pracovním právu jakožto soukromoprávní úpravě (pro vyloučení pochybností v dalším výkladu zůstávají stranou oblasti kolektivního pracovního práva a práva zaměstnanosti). Jedním z takových prvků též právě výše zmiňované omezení smluvní volnosti. Učebnice pracovního práva dokonce uvádí, že veřejnoprávní zásahy do občanských či obchodních vztahů představují zásadní odlišení od vztahů pracovněprávních.[144] Nikoliv méně významným veřejnoprávním rysem norem pracovního práva je dohled orgánů veřejné správy nad dodržováním vybraných norem pracovního práva. Tento dohled náleží úřadům práce, inspekci práce či jiným povolaným orgánům, které jsou oprávněny ukládat za porušení norem pracovního práva (za přestupky) příslušné sankce. To se samozřejmě týká i relevantních norem upravujících ochranu osobnosti zaměstnance.

Dalším specifickým rysem norem pracovního práva vyplývajícím z jejich částečně veřejnoprávního charakteru je zpravidla kogentní charakter norem pracovního práva. To je opět v zájmu ochrany zaměstnanců, aby nemohlo jednostranně z vůle dojít k vyloučení ustanovení sloužících jejich ochraně. Taková odchylná úprava by přitom byla možná pouze ve prospěch zaměstnance.[145] Kogentní normy se tak prolínají skrze celý zákoník práce, zejména je možné kogentní normy identifikovat v podstatě pro veškerá ustanovení určující minimální požadavky na pracovní podmínky (např. pracovní doba, doba odpočinku,

[144] Bělina, M. a kol. *Pracovní právo.* 7. doplněné a podstatně přepracované vydání 2017. Praha: C. H. Beck, 2017, s. 4-8.

[145] Srov. § 4a odst. 1 ZPr, podle kterého platí, že: „*Odchylná úprava práv nebo povinností v pracovněprávních vztazích nesmí být nižší nebo vyšší, než je právo nebo povinnost, které stanoví tento zákon nebo kolektivní smlouva jako nejméně nebo nejvýše přípustné*."

dovolená, mzda), dále též pro možnost jednostranného ukončení pracovní smlouvy ze strany zaměstnavatele, pro bezpečnost a ochranu zdraví při práci, ale i pro ochranu soukromí zaměstnance na pracovišti. Budeme-li se nicméně blíže zamýšlet nad kogentností ochrany osobnosti v pracovním právu, nutně dojdeme k závěru, že ta sama o sobě až takový přínos nemá, protože absolutní a tím i kogentní charakter norem chránících osobnost vyplývá již ze samostatné podstaty těchto norem.[146] Bez ohledu na tento závěr je nepochybné, že faktické zdvojení tohoto ochranného prvku není zaměstnancům na škodu, ale jen podtrhuje důležitost ochrany osobnosti zaměstnanců.

3.3 Legitimní očekávání soukromí

Legitimní či rozumné očekávání soukromí, v angličtině známé jako „*reasonable expectation of privacy*“, je důležitým konceptem, dalo by se říci východiskem, pro ochranu osobnosti a soukromí zaměstnanců na pracovišti. Tento právní test, jak bývá toto spojení označováno, není však sám o sobě výhradně spojen se vztahem zaměstnance a zaměstnavatele. Váže se na veškeré situace, kde lze očekávat jistou míru soukromí. Jako obecný příklad se nabízí uvést očekávání soukromí jedince v jeho domově. Vedle toho se však může tento test uplatnit například ve vztahu mezi zákazníkem a obchodníkem, mezi obchodními partnery a s určitými limity i na veřejnosti (například při ochraně před veřejným ponížením jakéhokoliv druhu). V dnešní době se s vývojem technologií tento koncept rozšiřuje též do prostředí internetu, kde se s ním lze setkat zejména u sociálních sítí (soukromý charakter konverzace vs. její zveřejnění apod.). V tomto ohledu naopak tradičním prostředím, kde lze očekávat určitou míru soukromí a kde je tento koncept aplikován, je právě pracoviště. Jelikož vychází tento test z judikatury, věnuje se tato podkapitola především rozboru příslušných soudních rozhodnutí.

Prvně byl koncept rozumného očekávání dovozován patrně na území Spojených států amerických v roce 1967 v rámci rozhodnutí Katz vs. Spojené státy.[147] Nebyl přitom vyjádřen v samotném rozhodnutí, ale v disentním stanovisku jednoho ze soudců. Přínos tohoto stanoviska spočívá ve vytvoření dvoustupňového testu rozumného očekávání soukromí, který je založen na tom, že za prvé jedinec vykazuje skutečné (subjektivní) očekávání soukromí a za druhé je jeho očekávání rozumné (ve smyslu toho, že společnost ho jako

[146] Srov. obecné ustanovení § 1 odst. 2 ObčZ zakotvující kogentní charakter norem pro ochranu osobnosti v celém soukromém právu.
[147] Solove, D. J., Schwartz, P. M. *Privacy Law Fundamentals*, Portsmouth: International Association of Privacy Professionals, 2017, s. 41.

rozumné přijímá).[148] Dalo by se tedy říci, že jde o průnik subjektivního vnímání soukromí s objektivním vnímáním stejného pojmu ze strany veřejnosti. Toto rozhodnutí, resp. právě disentní stanovisko, se nedlouho po svém vydání stalo v podstatě modlou ochrany soukromí na území Spojených států a dodnes je na ně odkazováno, a to nejen v souvislosti s ochranou soukromí, ale i jako na učebnicový příklad, kdy disentní stanovisko dokázalo v konečném důsledku převážit většinový názor.[149]

Na evropské půdě je v tomto ohledu klíčová judikatura ESLP, která se na rozumné očekávání soukromí mnohdy odkazuje při výkladu čl. 8 EÚLP. Za jedno z prvních rozhodnutí, v rámci kterých byl tento koncept použit, lze označit rozhodnutí ve věci *Halford vs. Spojené království*.[150] V rámci tohoto rozhodnutí posuzoval soud zákonnost odposlechů zaměstnankyně, která pracovala u policie a jejíž telefony, domácí i služební, byly odposlouchávány s cílem získat informace, které by mohly být použity v případných sporech. Soud v této věci dovodil, že v pozici stěžovatelky, paní Halfordové, bylo rozumné očekávat, že její telefony nebudou odposlouchávány. To skutkově odůvodnil tím, že měla k dispozici vlastní kancelář, kde byly k dispozici dva telefony, z nichž jeden byl určen pro její soukromé využití a prostřednictvím druhého bylo možné činit oznámení ohledně sexuální diskriminace. Očekávat soukromí bylo proto v její pozici rozumné, a to i z objektivního hlediska. Soud dal proto stěžovatelce za pravdu a přiznal jí odpovídající odškodnění.

Skutečnost, že odposlouchávání může a znamenat zásah do soukromí, byla následně potvrzena i v rozhodnutí *Amann v. Švýcarsko*.[151] Zajímavějším případem, kde byl však koncept rozumného očekávání dále použit, je případ *Copland vs. Spojené království*.[152] V této věci navázal ESLP na rozsudek Halford vs. Spojené království a dospěl k závěru, že telefonní hovory uskutečněné z obchodních prostor je nutné podřadit pod pojmy soukromý život a korespondence ve smyslu čl. 8 EÚLP. Tuto ochranu přitom soud vztáhl i na informaci o používání telefonu (volaná čísla, délka hovoru atd.), na e-mailovou korespondenci a na využívání internetu, když konstatoval, že nejen telefonické hovory mohou být součástí soukromého života, ale i internet a e-mailová komunikace. Získávání a shromažďování

[148] Winn, P. A. *Katz and the Origins of the „Reasonable Expectation of Privacy" Test*. McGeorge Law Review, Forthcoming, Vol. 40, Issue 1, 2009, s. 7 [online]. [cit. 2019-02-03]. Dostupné z: https://ssrn.com/abstract=1291870
[149] Tamtéž.
[150] Rozhodnutí ESLP ze dne 25. června 1997 ve věci Halford vs. Spojené království, č. stížnosti 20605/92.
[151] Rozhodnutí ESLP ze dne 16. února 2000 ve věci Amann vs. Švýcarsko, č. stížnosti 27798/95.
[152] Rozhodnutí ESLP ze dne 3. července 2007 ve věci Copland vs. Spojené království, č. stížnosti 62617/00.

příslušných informací bez vědomí stěžovatelky bylo proto zásahem do jejího soukromého života. Soud zde dovodil, že o takovéto skutečnosti nebyla informována, ale mohla ve svém postavení rozumně očekávat soukromí. Proto soud stěžovatelce opět přiznal odpovídající odškodnění.

Jak rozhodnutí ve věci Halford vs. Spojené království tak i Copland vs. Spojené království lze dnes již považovat za „klasiku", o které se lze dočíst ve většině knih věnujících se ochraně soukromí zaměstnanců. Na půdě ESLP lze nicméně identifikovat již značné množství obdobných rozhodnutí, které se věnují například sledování zaměstnanců kamerovými systémy. Jako příklad lze v tomto ohledu uvést rozhodnutí z nedávné doby ve věci *Akhlyustin vs. Rusko*,[153] kde soud dovodil, že zaměstnanec měl rozumné očekávání soukromí, protože nebyl informován o tom, že na pracovišti může být nahráván na (skrytou) kameru nebo, že jeho hovory mohou být odposlouchávány. Soud v této souvislosti vzal za důležité též skutečnost, že pořízené nahrávky byly dále uchovávány, zkoumány a využity jako důkaz v soudním řízení. Soud proto uzavřel, že využitím dotčených sledovacích zařízení došlo k porušení práva na ochranu soukromí ve smyslu čl. 8 EÚLP.[154]

Dalším z častěji citovaných rozhodnutí je rozhodnutí ve věci *Peev vs. Bulharsko*,[155] v rámci kterého byla posuzována přípustnost prohledání kanceláře ze strany nadřízených. Stěžovatel měl totiž ve své kanceláři připravený rezignační dopis, který se však rozhodl nepodat. Nicméně poté, co byl tento dopis v jeho šuplíku nalezen, nebyl již stěžovatel vpuštěn do své kanceláře. Soud v této věci jednoznačně shledal nutnost ochrany pro pracovní desku a šuplíky zaměstnance, kde tedy má zaměstnanec určitou míru rozumného očekávání soukromí (jiná by byla situace, pokud by bylo ze strany zaměstnavatele zakázáno mít na stole a v šuplících soukromé předměty). Soud dokonce naznačil, že by ochrana měla být poskytnuta celé kanceláři, dále však tato myšlenka rozvinuta nebyla. I tak byla tímto rozhodnutím ochrana zaměstnancova soukromí opět značně rozšířena.

Pokud jde o koncept legitimního očekávání soukromí, stojí ještě za zmínku nedávné rozhodnutí ve věci *Benedik vs. Slovinsko*.[156] To se sice netýká ochrany zaměstnance (šlo o případ policejního vyšetřování šíření dětské pornografie), je však zajímavé z hlediska toho,

---

[153] Rozhodnutí ESLP ze dne 5. března 2018 ve věci Akhlyustin vs. Rusko, č. stížnosti 21200/05.
[154] Obdobné závěry byly shledány též ve starším rozhodnutí ESLP o přípustnosti stížnosti ze dne 5. října 2010 ve věci Köpke vs. Německo, č. stížnosti 420/07, či v rozhodnutí ze dne 17. října 2003 ve věci Perry vs. Spojené království, č. stížnosti 63737/00 (toto se však netýkalo zaměstnance).
[155] Rozhodnutí ESLP ze dne 26. října 2007 ve věci Peev vs. Bulharsko, č. stížnosti 64209/01.
[156] Rozhodnutí ESLP ze dne 24. dubna 2018 ve věci Benedik vs. Slovinsko, č. stížnosti 62357/14.

ve kterých případech ještě lze dovozovat legitimní očekávání soukromí při využívání internetu. V daném případě šlo o to, zda je možné ochranu soukromí při využívání internetu dovozovat nejen ve vztahu k obsahu, ale též k provozním údajům jako je IP adresa, datum či jiné technické informace o přenosu dat. Soud ve svém rozhodnutí shledal, že i takovéto údaje podléhají ochraně. Aby tedy takové údaje mohly být pro účely vyšetřování použity, měla si policie v posuzovaném případě vyžádat soudní příkaz k jejich poskytnutí a požadované informace jí neměly být poskytnuty na základě pouhé (běžné) žádosti.

Z hlediska ochrany soukromí zaměstnance se s ohledem na toto rozhodnutí nabízí otázka, do jaké míry lze tuto ochranu týkající se provozních údajů při využívání internetu poměřit s právem zaměstnavatele přiměřeným způsobem kontrolovat, jakým způsobem jeho zaměstnanci využívají svěřené výrobní a pracovní prostředky ve smyslu § 316 odst. 1 ZPr. V rozhodnutí Kasalova pila[157] byla dovozena přípustnost použití provozních údajů jako důkazu, že zaměstnanec trávil většinu pracovní doby nepracovní činností na počítači. Je pak otázkou, zda by takové rozhodnutí obstálo ve světle výše uvedeného rozhodnutí ESLP ve věci Benedik vs. Slovinsko.

Spíše se lze domnívat, že ano, neboť jde o skutkově odlišné situace, kdy při obecném (anonymním) využívání internetu jednotlivce lze obecně očekávat vyšší míru soukromí. Naopak v situaci, kdy zaměstnanec nadužívá svěřené pracovní prostředky zaměstnavatele způsobem, který je ze strany zaměstnavatele zakázán, by toto očekávání mělo být obecně nižší. Ve smyslu testu legitimního očekávání soukromí by však zaměstnanec měl být o možnosti kontroly a způsobech jejího provádění vždy informován (a to přestože půjde „jen“ o kontrolu dle § 316 odst. 1, nikoliv o sledování dle § 316 odst. 2 zákoníku práce). Jiný výklad by totiž v podstatě paralyzoval jakoukoliv možnost zákonného provádění kontrol ze strany zaměstnavatelů ve smyslu § 316 odst. 1 zákoníku práce.

V této práci však není prostor, aby byla blíže popisována všechna rozhodnutí. Bližší pozornost si však zaslouží určitý posun, který je možné spatřovat v judikatuře ESLP a který je popsán v další podkapitole.

3.4 Ochrana, i když není rozumné očekávat soukromí

Jak bylo naznačeno výše, judikatura se postupem času vyvíjí, a to nejen tím, jak je chápán test legitimního očekávání soukromí a kdy je nutné jej aplikovat, ale postupně

[157] Rozhodnutí Nejvyššího soudu ČR ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011.

dochází také k dovozování ochrany i na případy, kdy by objektivně nemělo být soukromí očekáváno. V rámci judikatury ESLP týkající se ochrany zaměstnanců je toto zcela patrné na nedávném rozhodnutí ve věci *Barbulescu vs. Rumunsko*,[158] tedy rozhodnutí Velkého senátu ESLP, kterým bylo zrušeno předchozího rozhodnutí senátu čtvrté sekce ESLP v téže věci. V dané věci šlo o situaci, kdy zaměstnavatel na základě monitorování aktivit svého zaměstnance zjistil, že zaměstnanec užíval pracovní počítač pro účely soukromé komunikace.[159]

Senát ESLP ve svém rozhodnutí ze dne 12. ledna 2016 dovodil, že v pozici zaměstnance nebylo rozumné očekávat soukromí ve vztahu ke komunikaci prováděné prostřednictvím zaměstnavatelova komunikačního nástroje. Zároveň se odlišil od rozhodnutí ve výše zmíněných věcech *Halfrod a Copland*, kdy bylo použití služebních komunikačních nástrojů pro soukromé potřeby dovoleno, resp. tolerováno. Toto ale tentokrát v posuzovaném případě neplatilo, jelikož zaměstnanec byl informován o tom, že daný komunikační nástroj je monitorován a že zaměstnanec není oprávněn jej používat pro soukromé účely. Obdobně se odlišil od výše zmíněného rozhodnutí ve věci *Peev vs. Bulharsko*, neboť v daném případě také nebyl žádný předpis, který by zaměstnancům zakazoval mít na pracovišti své osobní předměty.

Stěžovatel nicméně následně využil svého práva předložit věc velkému senátu ESLP a ten posunul ochranu soukromí zaměstnanců ještě dále, když v podstatě vyslovil, že zaměstnance nelze zcela zbavit práva na ochranu soukromí na pracovišti, respektive že nelze snížit ochranu jeho soukromí na nulu. Předně totiž platí, že jakákoliv komunikace zaměstnance (prostřednictvím jakéhokoliv nástroje) bude spadat pod koncept ochrany korespondence, a to i přesto, že se odehrává na cizím (zaměstnavatelově) zařízení. Není ani rozhodné, že zaměstnanec byl na možný monitoring upozorněn. Z hlediska výkladu o rozumném očekávání soukromí zaměstnance je proto přinejmenším diskutabilní, zda toto očekávání zaměstnanec měl a vůbec mohl mít, když byl o možných kontrolách (údajně) informován. Samotný Velký senát ESLP ponechal odpověď na tuto otázku otevřenou, byť je zřejmé, že sám měl o jakémkoliv rozumném očekávání soukromí ze strany zaměstnance velké pochybnosti. Každopádně ani toto nebylo na újmu tomu, aby zaměstnanci byla v dané věci přiznána ochrana.

Skutečnost, že tyto závěry nebyly nějakým dočasným úskokem v judikatorním rozhodování, byla již potvrzena i v dalším rozhodnutí, a to ve věci Antonović a Mirković

[158] Rozhodnutí ESLP ze dne 5. září 2017 ve věci Barbulescu vs. Rumunsko, č. stížnosti 61496/08.
[159] Blíže k danému rozhodnutí srov. Zahradníček, J. *Sledování elektronických komunikací na pracovišti*. Právní rádce. 2016, 50-55.

vs. Černá hora.[160] V tomto případě bylo opět posuzováno využití kamerových systémů na univerzitě, resp. na pracovišti, a soud shledal, že nelze omezit soukromý (sociální) život na nulu a je nerozhodné, že šlo o nikoliv skryté, ale otevřené sledování na pracovišti, o kterém byli všichni informováni, a že zaměstnavatelovy vnitřní předpisy byly velmi restriktivní. I přesto je nutné chránit soukromí, ačkoliv to může být za určitých podmínek legitimně omezováno.[161]

Tato obě rozhodnutí ve věcech Barbulescu a Antonović a Mirković nepochybně posouvají ochranu zaměstnanců ještě dále za koncept legitimního očekávání soukromí. Z právního hlediska by měla být interpretována především s ohledem na charakter právních norem ochrany osobnosti a soukromí. Jejich absolutní povaha totiž nedává obecně nikomu možnost je omezit či zcela vyloučit, natož zaměstnavateli, který je v silnějším postavení vůči zaměstnancům. Naopak koncept rozumného očekávání soukromí vychází ze samotné skutkové podstaty ochrany soukromí. Je tedy jednou z jeho imanentních součástí. Oba zmíněné fenomény, jak legitimní očekávání soukromí, tak i nemožnost snížit ochranu soukromí v určitých případech na nulu, se přitom v závislosti na skutkových okolnostech mohou prolínat a ve svém výsledku poskytovat zaměstnancům neomezitelnou minimální úroveň soukromí, kterou může každý zaměstnanec očekávat a která se uplatní téměř vždy. Samozřejmě vždy záleží na konkrétních skutkových okolnostech, ale již je nepochybné, že sebelepší plnění informační povinnosti zaměstnavatelů vůči svým zaměstnancům nemusí mít žádný význam. Dochází tak k judikatorní reflexi slabšího postavení zaměstnance s ohledem na rozvoj technologií a nástrojů, které dnes zaměstnavatelé využívají ke sledování svých zaměstnanců, a to ve vztahu k ochraně soukromého a sociálního života osob (zaměstnanců) jakožto absolutního práva.

S nadsázkou lze říci, že bez této ochrany a s uznáním plného práva zaměstnavatele své zaměstnance kontrolovat by se ze zaměstnanců stali otroci. S ohledem na to lze tento judikatorní posun ESLP hodnotit jednoznačně pozitivně. Na druhou stranu výše uvedené značně komplikuje situaci zaměstnavatelům, kteří ve stínu těchto rozhodnutí v podstatě nemohou mít definitivní jistotu o tom, že využívané kontrolní a sledovací mechanismy nezasahují nad míru do práva na ochranu soukromí zaměstnanců, a to na vzdory tomu, že zaměstnance o způsobech a rozsahu kontrol řádně informují. Nabízí se proto otázka, zda by přece jen nebylo do budoucna vhodné legislativně blíže vymezit podmínky využívání jednotlivých (v praxi nejčastěji používaných)

[160] Rozhodnutí ESLP ze dne 28. listopadu 2017 ve věci Antonović a Mirković vs. Černá hora, č. stížnosti 70838/13.

[161] Za pozornost také stojí, že soud vyzdvihuje skutečnost, že univerzita není jen místo, kde dochází k výuce studentů, ale také k jejich vzájemné interakci, tudíž k rozvoji jejich vzájemných vztahů a rozvoji sociální identity. Nepochybně tak naznačil, že i takovéto prostředí je hodno ochrany, obdobně jako pracoviště, a lez v jeho rámci mít určitou míru rozumného očekávání soukromí.

nástrojů, jako jsou kamery, odposlouchávací nástroje, nástroje pro sledování využívání počítačů apod., aby zaměstnavatelé i zaměstnanci měli vyšší právní jistotu ohledně svého postavení.

4 Ochrana osobnosti zaměstnanců v čase

Záměrem této kapitoly je analyzovat ochranu osobnosti zaměstnance v různých fázích jeho vztahu se zaměstnavatelem, a to z hlediska ochrany před vznikem pracovního poměru, v době jeho trvání a po skončení pracovního poměru. Vzhledem k tomu, že ochrana osobnosti v době trvání pracovního poměru je blíže zkoumána v rámci samostatné kapitoly 5, je v této kapitole specificky rozebrána pouze ochrana osobnosti v ostatních dvou časových úsecích. Cílem tedy je blíže identifikovat relevantní platnou právní úpravu, zanalyzovat ji, pokud existuje, a zhodnotit její pozitiva i negativa při praktické aplikaci.

Relativně samostatnou částí této kapitoly je také zamyšlení nad ochranou osobnosti v rámci jednoho dne, a to ve smyslu srovnání ochrany osobnosti v době, kdy je zaměstnanec na pracovišti, kdy vykonává práci, kdy je doma po skončení pracovní doby ve svém volnu, kdy případně vykonává tzv. home office či jiné flexibilní formy výkonu práce.

4.1 Ochrana před vznikem pracovního poměru

O ochraně osobnosti je nepochybně relevantní mluvit ještě před vznikem pracovního poměru, a to v době, kdy se jedinec uchází o zaměstnání. Je pochopitelné, že zaměstnavatelé mají nárok na to, aby si mohli uchazeče o zaměstnání prověřit, zejména z toho ohledu, zda zaměstnanec je dostatečně způsobilý vykonávat požadovanou práci. Zvlášť když je uchazeč po vzniku pracovního vztahu ze strany norem pracovního práva značně zvýhodňován. Nicméně i pro toto prověřování musí existovat určité mantinely. Jednak má zaměstnavatel možnost uchazeče o zaměstnání zčásti poznat již na osobním pohovoru, může si prověřit dosažené vzdělání zaměstnance a může ho požádat o prokázání dosažené praxe, vedle toho si může zaměstnancovu způsobilost dostatečně prověřit v rámci zkušební doby, která mu umožňuje zaměstnanci kdykoliv bezdůvodně pracovní poměr zrušit.[162]

Je proto zřejmé, že jednostranné prověřování uchazeče o zaměstnání ze strany zaměstnavatele musí mít určité hranice. Obzvláště to platí v dnešní době, kdy rozmach informačních technologií učinil jakékoliv prověřování ze strany zaměstnavatelů velmi snadným. Příkladem mohou být sociální sítě, které se zaměstnavatelé naučili využívat (a zneužívat) proti zaměstnancům. Situace je dnes už dokonce tak daleko, že obdobné jednání, totiž systematická lustrace uchazečů o zaměstnání, je považováno za standard. V anglicky mluvících zemích se pro tyto činnosti uchytilo slovní spojení „background

[162] Srov. ustanovení § 66 Zpr.

check“. Pokud je takové jednání prováděno s vědomím a svolením zaměstnance, na základě informací zaměstnancem poskytnutých, není třeba v tomto vidět větší problém. Co když ale zaměstnavatel takové jednání provádí bez vědomí uchazeče o zaměstnání a vyžaduje nebo vyhledává informace, které by vyžadovat neměl? Že nejde o smyšlený problém, dokládá i skutečnost, že na tuto negativní praxi poukazuje WP29, která výslovně uvádí, že není důvod pro to, aby zaměstnavatel požadoval od uchazečů přístup k jejich profilům na sociálních sítích.[163]

4.1.1 Pohled do zahraničí

Pokud jde o provádění důkladných „*background checks*“, je extrémním příkladem situace v USA, kde je praxe prověřování si uchazečů o zaměstnání na denním pořádku. Na úvod a pro lepší pochopení je vhodné si položit několik otázek k zamyšlení. Je v pořádku, aby uchazečka o zaměstnání nebyla přijata na pozici učitelky, jelikož na svém účtu na síti MySpace umístila svou fotku s pirátským kloboukem na hlavě, když pila z plastového kelímku? Nebo když uchazeč na svém facebookovém účtu vyjadřuje své poltické názory, které nejsou v souladu s politickými názory zaměstnavatele? V USA jde o zcela běžné případy.[164] Může jít přitom mnohdy o nevinné případy, kdy střízlivý řidič vozidla bude vyfocen, jak drží alkohol, a následně jeho fotografie bude umístěna na sociální síť.[165]

Dalo by se jistě říci, že uchazeč má do určité míry vždy možnost své soukromí si chránit. Sociální sítě dnes nabízejí řadu nastavení, která umožňují sdílení informací omezit jen vůči určitým osobám. Ale ani to bohužel nemusí být dostatečné. V USA byly běžné případy, kdy uchazeči o zaměstnání byli v rámci pohovoru požádání o sdělení hesla ke svým přístupovým účtům do sociálních sítí.[166] Vedle toho uchazeč o zaměstnání nebude uchráněn ani v případě, pokud bude zaměstnavatel znát někoho, kdo mít přístup k informacím bude (například někteří spoluzaměstnanci). Jakékoliv ad hoc účelové opatření ze strany uchazeče o zaměstnání před pohovorem bude dále bezvýznamné v situacích, kdy on sám práci nevyhledává, ale jiný zaměstnavatel se sám poohlíží po nových zaměstnancích a oslovuje je (v této situaci by tedy potenciální zaměstnanec ani osloven nebyl). Navíc se snadno může stát, že se k účtu dostane někdo neoprávněný, kdo na něm uveřejní například rasistické

[163] Srov. stanovisko WP29 č. 2/2017: Zpracování údajů na pracovišti (v originále: *opinion 2/2017 on data processing at work*). (WP249), ze dne 8. června 2017.
[164] Blíže viz též Vroman, M., Stulz, K., Hart, C., Stulz, E. *Employer Liability for Using Social Media in Hiring Decisions*. Journal Social Media for Organizations, 2016, Vol. 3, Issue 1, s. 2-3.
[165] Op. cit. sub. 85, s. 56.
[166] Tamtéž, s. 76.

výroky – činí tato skutečnost následně vlastníka účtu rasistou? Je zřejmé, že ne, ale pro potenciálního zaměstnavatele může tato zjištěná skutečnost dostatečně odůvodňovat proč uchazeče o zaměstnání na pohovor ani nepozvat, aniž ten by se dozvěděl důvody a měl možnost se proti tomu bránit. Problémem takto získaných informací samozřejmě také je, že nejsou či nemusí být věrohodné a je velmi obtížné ověřit jejich pravost (chytrý uchazeč toho samozřejmě může využít též ve svůj prospěch).

Výše uvedené problémy nejsou jen hypotetické. V USA se uvádí, že sedmdesát pět procent společností požaduje po svých náborářích, aby tyto informace vyhledávali, a až sedmdesát procent kandidátů je odmítnuto právě na základě informací dohledaných online.[167] Ano, situace v USA a situace ve většině zemí Evropské unie se do značné míry liší. V USA je v podstatě dovozováno, že zaměstnanec vyměňuje své soukromí se zaměstnavatelem za nabídku práce.[168] Na základě toho je pak zaměstnavatel oprávněn zasahovat do jeho soukromí a nic mu ani nebrání si zaměstnance důkladně prověřit před nabídkou práce, ať už informace získává kdekoliv (včetně sociálních sítí).[169] Dokonce situace jde tak daleko, že pokud si zaměstnavatel o uchazeči dohledá určité „negativní" informace a ignoruje je, může z toho být následně vyvozována odpovědnost zaměstnavatele, pokud daný zaměstnanec následně způsobí škodu (například zákazníkovi).[170]

Je nicméně zřejmé, že situace v Evropě (alespoň ve většině zemí) se odlišuje. Na rozdíl od závěru, že jedinec dává zaměstnavateli své soukromí výměnou za vyplácení mzdy, se v Evropě více prosazuje ochranné zákonodárství, které garantuje relativně silnou ochranu zaměstnance i v rámci zaměstnání. Na rozdíl od USA je dovozováno, že ochrana soukromí je úzce spojena s důstojností člověka, která je člověku přiznána společností, a z toho důvodu nemůže být jednoduše směněna za jiná práva.[171] Podle autora této práce tato skutečnost vychází především ze skutečnosti, že ochrana osobnosti, včetně ochrany soukromí, je absolutní povahy a možnosti limitace tohoto práva jsou velmi omezené.[172]

---

[167] Sanders, S. D. *Privacy is Dead: The Birth of Social Media Background Checks*. Southern University Law Center REV. 24, 2012, s. 18 [online]. [cit. 2019-02-05]. Dostupné z: https://ssrn.com/abstract=2020790
[168] Suder, S. *Pre-employment Background Checks on Social Networking Sites - may your boss be watching?* Masaryk University Journal of Law and Technology, 2014, Vol. 8:1, s. 127.
[169] Tamtéž.
[170] Srov. Davison, H. K., Maraist, C.C., Hamilton, R. H., Bing, M.N. *To Screen or Not to Screen? Using the Internet for Selection Decisions*. Employee Responsibilities and Rights Journal, 2012, vol. 24, no. 1, s. 8 [online]. [cit. 2019-02-05]. Dostupné z: https://www.academia.edu/10086027/To_Screen_or_Not_to_Screen_Using_the_Internet_for_Selection_Decisions
[171] Op. cit. sub. 168, s. 128.
[172] Srov. blíže výklad v bodě 2.1.5.

Kde je však hranice v případě uchazečů o zaměstnání? Mohou si zaměstnavatelé v Evropě vyhledávat, kde chtějí a co chtějí? Nebo nesmí naopak nic? Odpovědět na tyto otázky není jednoduché. Předně je třeba uvažovat skutečnost, že jedinec se chtě nechtě zčásti vzdává ochrany svého soukromí, pokud učiní nějaké informace o své osobě volně přístupnými. Naopak pokud takové informace šíří v rámci úzkého okruhu osob, patrně by mu bylo možné přiznat určitou míru rozumného očekávání soukromí[173] a jakékoliv využití takovýchto informací nepovolanými osobami by mělo být považováno za nedovolené. Konečné rozhodnutí o dovolenosti či nedovolenosti využití informací však bude pravděpodobně možné učinit až v závislosti na posouzení konkrétních skutkových okolností.

Některé evropské státy se alespoň do určité míry snaží tuto otázku uchopit a nabídnout vodítka k tomu, kde leží tato hranice mezi ochranou soukromí zaměstnance a právem zaměstnavatele si budoucího zaměstnance prověřit. Příkladem jsou zejména Velká Británie, Německo a především Finsko[174] (ve Velké Británii a Německu jsou tyto spíše na úrovni soft law).[175] Zejména Finsko je velmi napřed, pokud jde o ochranu soukromí zaměstnanců. Ve Finsku je totiž platný zvláštní zákon na ochranu soukromí v pracovním životě, který ve svém článku 4 určuje, že zaměstnavatel má informace o zaměstnanci shromažďovat v první řadě od něj. Pokud by informace (osobní údaje) chtěl získávat odjinud, musí k tomu mít předchozí souhlas zaměstnance. Na základě těchto ustanovení dokonce rozhodl finský ombudsman na ochranu osobních údajů, že zaměstnavatelé nejsou oprávněni při prověřování uchazečů o zaměstnání využívat vyhledávací nástroje, jako je například Google.[176] Tyto závěry tak bude možné nepochybně vztáhnout i na využívání a dohledávání informací na sociálních sítích či jinými způsoby online. Ochraně soukromí zaměstnanců je tak přiznávána velká váha. K zamyšlení je nicméně otázka, do jaké míry jsou tyto normy v praxi skutečně vymahatelné – je opravdu možné zabránit zaměstnavateli, aby si zapnul internet a danou osobu si prolustroval? Kdo mu v tom prakticky zabrání a jak mu bude možné toto prokázat? To jsou otázky, které do značné míry zpochybňují význam této úpravy, nicméně alespoň z hodnotového hlediska lze jejich existenci nepochybně hodnotit kladně.

---

[173] Srov. výklad v bodě 3.3.
[174] Op. cit. sub. 168, s. 129 až 132.
[175] Bližší pohled do vybraných zahraničních právní úprav viz podkapitola 9.1.
[176] Kennedy, N., Macko, M. *Social Networking Privacy and Its Effects on Employment Opportunities*. The information age, 2, 111–23. 2009. [online]. [cit. 2019-02-06]. Dostupné z: http://www.ethicapublishing.com/inconvenientorinvasive/2CH12.pdf

4.1.2 Situace v ČR

Český právní řád na ochranu osobnosti uchazečů o zaměstnaní také myslí. Přestože se nemůže mírou detailu srovnávat s finskou právní úpravou, ani v ČR si zaměstnavatel nemůže dovolit dělat cokoliv. Odhlédneme-li pro tuto chvíli od právní úpravy ochrany osobních údajů, je z hlediska platné právní úpravy důležité zejména ustanovení § 30 odst. 2 ZPr, podle kterého platí, že *„zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci, nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy“*. Tím je do zákoníku práce jednoznačně vtěleno, že zaměstnavatel může od zaměstnanců vyžadovat jen relevantní informace. Chybí nicméně již bližší rozlišení toho, co lze považovat za relevantní informace a co nikoliv. Rovněž zcela chybí úprava toho, zda a za jakých podmínek je zaměstnavatel oprávněn vyhledávat a využívat informace o uchazeči bez jeho přispění.

Pokud jde o určení toho, co je a co není relevantní informace, lze se přece jen částečně inspirovat v zákoně. Ustanovení § 316 odst. 4 ZPr totiž vymezuje údaje, které zaměstnavatel nesmí po zaměstnancích vyžadovat. Zakázáno je vyžadování informací, které bezprostředně nesouvisí s výkonem práce a se základním pracovněprávním vztahem. To by nás ve výkladu příliš dále neposunulo, v ustanovení je nicméně dále uveden demonstrativní výčet takovýchto informací, které zaměstnavatel nemůže vyžadovat. Jedná se o informace o těhotenství, rodinných a majetkových poměrech, sexuální orientaci, původu, členství v odborové organizaci, členství v politických stranách nebo hnutích, příslušnosti k církvi nebo náboženské společnosti a o trestněprávní bezúhonnosti.[177] V teorii je přitom nepochybné, že pokud zákon zakazuje získávání těchto informací v rámci pracovního poměru, je logické jej aplikovat i na osoby ucházející se o zaměstnání.[178] Naopak je třeba konstatovat, že tyto informace budou zaměstnavatele obvykle zajímat právě ještě před započetím pracovněprávního vztahu, a proto je potřebné ochranu poskytovanou tímto ustanovením aplikovat i na uchazeče o zaměstnání a na požadování údajů zaměstnavatelem před vznikem pracovního poměru ve smyslu § 30 odst. 2 ZPr.

Z ustanovení § 316 odst. 4 ZPr nicméně platí výjimky týkající se možnosti požadovat tam demonstrativně vyjmenované údaje. Zaměstnavatel je totiž oprávněn část z těchto údajů

[177] Stranou je teď ponechán výklad ke skutečnosti, že tyto údaje jsou mnohdy i nadále vyžadovány v rámci standardizovaných dotazníků využívaných ještě v dobách před přijetím Zpr.
[178] Srov. Štefko in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1246.

(údaje dle § 316 odst. 4 písm. písm. a), b) a h) ZPr)[179] vyžadovat, je-li to *„pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený“.*[180] Skutečnosti, co je věcný důvodem spočívajícím v povaze páce a kdy bude takovýto požadavek přiměřený, jasně definovány nejsou. Podle názoru autora této práce by však s jejich určováním neměl být větší problém. Bude vždy samozřejmě záviset na konkrétních skutkových okolnostech. Ty by však měly být dobře odvoditelné (a zpětně ověřitelné) podle náplně práce, o kterou se jedinec uchází a kterou vykonává. Není proto v odborné literatuře[181] ani v praxi pochyb, pokud zaměstnavatel například vyžaduje doložení skutečnosti, že zaměstnanec nebyl trestně odsouzen za majetkovou činnost, jestliže mu má být v rámci výkonu pracovní pozice svěřen větší obnos, nebo že nebyl odsouzen za trestný čin související s výrobou, přechováním či jiným nakládáním s omamnými a psychotropními látkami, když by v rámci výkonu pracovní pozice měl mít přístup právě k takovýmto látkám. Obdobně u pracovní pozice, která je fyzicky náročná a která zahrnuje práci ve ztížených pracovních podmínkách či v noci, má zaměstnavatel nárok být informován o případném těhotenství uchazečky. K situaci, kdy by zaměstnavatel byl oprávněn požadovat informace o majetkových poměrech zaměstnance, by mohlo dojít například tehdy, pokud by bylo potřeba prověřit zaměstnancův případný střet zájmů a hrozilo by vysoké riziko na zneužití pravomoci či informací, přičemž toto by nebylo možné kontrolovat jiným způsobem (v žádném případě by však nemělo docházet k suplování úkolů, kterými je pověřena Policie České republiky či jiné příslušné orgány veřejné správy).

Ani vůči požadování ostatních údajů[182] však neplatní absolutní zákaz a je možné je (i ostatní údaje zmíněné v § 316 odst. 4 ZPr) požadovat v případech, kdy tak stanoví ZPr nebo zvláštní právní předpis. Ač není legislativně technická metoda zvolená v rámci ustanovení § 316 odst. 4 ZPr nejšťastnější a mohla by připouštět též výklad, že část údajů dle § 316 odst. 4 ZPr není možné požadovat nikdy, je nutné podle názoru autora této práce takový výklad odmítnout a dojít k závěru, že žádný ze zmíněných údajů nemá zcela absolutní

[179] Tj. údaje o těhotenství, rodinných a majetkových poměrech a trestněprávní bezúhonnosti.
[180] § 316 odst. 4 ZPr.
[181] Op. cit. sub. 178 nebo Morávek in Pichrt, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. Praha: Wolters Kluwer, 2017, s. 958.
[182] Údaje o sexuální orientaci, původu, členství v odborové organizaci, členství v politických stranách a hnutích a údaje o příslušnosti k církvi nebo náboženské společnosti.

ochranu.[183] Je totiž nepochybné, že i ony „zapovězené“ údaje mohou být někdy stanoveny jako legitimní podmínka pro uchazeče o zaměstnání.

Přestože je výčet uvedený v § 316 odst. 4 ZPr demonstrativní, není příliš jasné, jaké další údaje by neměl být zaměstnavatel oprávněn vyžadovat. Patrně by se v tomto ohledu dalo inspirovat ustanoveními, která mají obdobný charakter. Jednak by tedy mohlo jít o ustanovení článku 9 odst. 1 nařízení GDPR, které vymezuje zvláštní kategorie osobních údajů (citlivé osobní údaje ve smyslu starší terminologie). Tyto kategorie mají obdobný charakter a nad rámec ustanovení § 316 odst. 4 ZPr uvádí genetické údaje, biometrické údaje a údaje o zdravotním stavu.[184] Genetické a biometrické údaje asi příliš relevantní ve vztahu k uchazečům (nikoliv zaměstnancům) nebudou, ale údaje o zdravotním stavu jistě svůj význam mají. Ačkoliv se na tyto údaje bezpochyby mnohdy také bude aplikovat výjimka uvedená v předchozím odstavci, nemusí tomu tak být vždy a zaměstnavatel rozhodně není oprávněn tyto údaje vyžadovat bezdůvodně.[185]

4.1.3 Zákon o zaměstnanosti

Dalším obdobným ustanovením, na základě kterého je možné rozvést demonstrativní výčet uvedený v § 316 odst. 4 ZPr, ale které má zároveň i samostatný význam pro možnost vyžadovat určité informace od uchazeče o zaměstnání, je ustanovení § 12 odst. 2 zákona č. 435/2004 sb., o zaměstnanosti, ve znění pozdějších předpisů (dále jen „ZoZ“). Toto ustanovení, podobně jako ustanovení § 30 odst. 2 ZPr míří na možnost, či spíše zákaz zaměstnavatele vyžadovat určité informace od uchazečů o zaměstnání. Jde však dále a uvádí konkrétní údaje, které není možné v takové situaci chtít. Tento výčet je do značné míry podobný výčtu uvedenému v § 316 odst. 4 ZPr, navíc je explicitně zmíněn zákaz vyžadovat údaje o národnosti, je specifikován původ, který není možné požadovat (rasový či etnický), a je zmíněno navíc filozofické přesvědčení. Z tohoto hlediska se proto zdá být přínos tohoto ustanovení značně mizivý, a to i z hlediska toho, že zákaz vyžadovat příslušné uvedené informace platí jen, pokud by jejich vyžadování nebylo v souladu s ustanoveními zákona č. 198/2009 Sb., antidiskriminační zákon, ve znění pozdějších předpisů (dále jen „AntidZ“). Toto ustanovení tedy jen zdůrazňuje povinnost AntidZ aplikovat, aniž by mělo samo věcný

[183] Na nevhodnost zvolených ustanovení poukazuje Štefko in Odlišně Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1246, který takovou možnost dovozuje pouze pro dotazování se na náboženské vyznání v případě církví.
[184] V ostatním jsou uvedené údaje obdobné jako v případě § 316 odst. 4 ZPr (nikoliv totožné).
[185] Blíže k otázkám zpracování těchto osobních údajů srov. podkapitola 7.4.

přínos. Přínosem by snad mohlo být, že zakázáno je též vyžadovat *„informace, které odporují dobrým mravům, a osobní údaje, které neslouží k plnění povinností zaměstnavatele stanovených zvláštním právním předpisem“.*[186] I tento zákaz by však bylo možné dovodit výkladem, ať už z obecného principu ochrany dobrých mravů či z výše zmíněného § 30 odst. 2 ZPr.

Podle § 12 odst. 2 ZoZ také platí, že *„na žádost uchazeče o zaměstnání je zaměstnavatel povinen prokázat potřebnost požadovaného osobního údaje“*. Podle názorů autora této práce však není ani v tomto ustanovení velký věcný přínos, jelikož jen stěží se bude zaměstnanec takové ochrany domáhat v situaci, kdy se jako slabší strana uchází o zaměstnání a snaží se zaměstnavateli zalíbit v konkurenci ostatních zaměstnanců (to samozřejmě neplatí, pokud by vyžadování takového údaje mohlo mít diskriminační charakter, kde by jistě bylo možné se ochrany domáhat snáze). Autor této práce proto považuje význam ustanovení § 12 odst. 2 ZoZ spíše za hodnotový. Ač svým textem opakuje skutečnosti, které by bylo z větší části možné dovodit z jiných ustanovení či výkladem, podtrhuje a zdůrazňuje ochranu osobnosti zaměstnance jakožto hodnotu, kterou tyto předpisy (ZoZ a ZPr) opakovaně vyjadřují, a snaží se tím zajistit, aby došlo alespoň k částečnému vyvážení postavení zaměstnance a zaměstnavatele.

4.1.4 Antidiskriminační zákon

Pokud jde o vyžadování určitých informací a pravidla zákazu diskriminace, platí předně ustanovení § 4 odst. 2 ZoZ, které v obecné rovině zakotvuje zákaz diskriminace při uplatňování práva na zaměstnání. Ač dané ustanovení dále uvádí výčet důvodů, proč nelze zaměstnanci odepřít zaměstnání, je tento výčet širší než výčet údajů uvedených v § 12 odst. 2 ZoZ či § 316 odst. 4 ZPr, neboť obsahuje též některé informace, které naopak zaměstnavatel může legitimně (téměř vždy) požadovat, zejména jazyk. Další „zapovězené“ informace tak v tomto ustanovení spíše hledat nelze. Pokud jde o již zmiňovaný AntidZ, ten především určuje, jaké jsou přípustné formy rozdílného zacházení. Ve vztahu k větší části výše zmíněných údajů je přitom určeno, že na jejich vyžadování lze založit rozdílné zacházení, pokud je toto rozdílné zacházení objektivně odůvodněno legitimním cílem a prostředky k jeho dosažení jsou přiměřené a nezbytné.[187] Ve věcech práva na zaměstnání je pak podle

[186] Srov. § 12 odst. 2 ZoZ.
[187] Jedná se o údaje o pohlaví, sexuální orientace, věku, zdravotního postižení, náboženského vyznání, víry či světového názoru (srov. ustanovení § 7 ZoZ).

§ 6 odst. 3 možné rozdílné zacházení založit (a příslušné údaje vyžadovat), je-li k tomu věcný důvod spočívající v povaze vykonávané práce nebo činnosti a uplatněné požadavky jsou této povaze přiměřené.[188] V případě závislé práce vykonávané v církvích nebo náboženských společnostech o diskriminaci podle § 6 odst. 4 nepůjde, pokud z povahy těchto činností nebo souvislosti, v níž jsou vykonávány, představuje náboženské vyznání, víra či světový názor osoby podstatný, oprávněný a odůvodněný požadavek zaměstnání se zřetelem k etice dané církve či náboženské společnosti.[189]

Vztah výše zmíněných ustanovení AntidZ a § 316 odst. 4 ZPr bohužel není příliš jasný. Ač ustanovení § 316 odst. 4 ZPr dovoluje vyžadovat ony „zapovězené" informace, stanoví-li tak zvláštní předpis, AntidZ neříká, že je takové údaje možné vyžadovat, ale pouze uvádí, že je možné na takových údajích založit rozdílné zacházení. V komentářové literatuře se lze dočíst, že AntidZ tímto nepřímo novelizoval ustanovení § 316 odst. 4 ZPr.[190] Bohužel opravdu jen nepřímo. Dnes tak nepochybně lze dovozovat, že údaje o příslušnosti k církvi nebo náboženské společnosti bude možné vyžadovat za podmínek uvedených v § 6 odst. 4 ZoZ. Už ale není zřejmé, kdy se zaměstnavatel bude moci ptát na údaje o sexuální orientaci zaměstnance, jeho původu, členství v odborové organizaci či členství v politických stranách nebo hnutích. Nepochybně to bude možné, pokud tak explicitně stanoví právní předpis. Bude ale možné na tyto informace aplikovat AntidZ a dovodit, že je možné tyto informace požadovat, pokud je k tomu věcný důvod spočívající v povaze vykonávané práce nebo činnosti a uplatněné požadavky jsou této povaze přiměřené? Pokud ano, má potom vůbec nějaký význam ochrana zakotvená v ustanovení § 316 odst. 4 ZPr? Analýzou právní úpravy není odpověď na tyto otázky zřejmá. Autor této práce se přitom spíše kloní k závěru, že kromě informací o příslušnosti k církvi nebo náboženské společnosti (kde je výjimka v AntidZ dostatečně konkrétní, tj. jde o zvláštní ustanovení), nelze v ostatním AntidZ na požadování informací podle § 316 odst. 4 ZPr aplikovat. Nepochybně by ale bylo vhodné daná ustanovení novelizovat a jejich vzájemný vztah vyjasnit.

[188] Srov. ustanovení § 6 odst. 3 ZoZ.
[189] Srov. ustanovení § 6 odst. 4 ZoZ.
[190] Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1246. Ke stejným závěrům o možnosti překonání zákazu dle § 316 odst. 4 dochází též Morávek (Morávek in Pichrt, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. Praha: Wolters Kluwer, 2017, s. 958.).

4.1.5 Shrnutí

Česká právní úprava určitou ochranu osobnosti uchazečům nepochybně poskytuje. Podle autora této práce je však tato ochrana v dnešní době již příliš úzce zaměřena a není dostačující. Předně není nijak reagováno na možnosti získávání informací ze strany zaměstnavatelů od třetích stran.[191] Ačkoliv poslední věta ustanovení § 316 odst. 4 ZPr uvádí, že *„tyto informace nesmí zaměstnavatel získávat ani prostřednictvím třetích osob“*, bude obtížné toto pravidlo dovozovat na jiné než tam uvedené informace (přestože není pochyb o tom, že uvedený výčet je demonstrativní).

Problematické bude právě získávání informací obecně z internetových stránek a ze sociálních sítí. Snad by v pozici uchazeče o zaměstnání bylo možné alespoň se bránit s odkazem již popisovaný princip rozumného očekávání soukromí, pokud by získané informace byly získány zásahem do zaměstnancova soukromí. Co by ale bylo zásahem takové intenzity, zřejmé není. Nemluvě o zaměstnancově možnosti či spíše nemožnosti prokázat, že tyto informace byly takovým způsobem získány. To je však obecným problémem, který legislativa sama o sobě zvládne vyřešit jen obtížně.[192] Nemusí to být ale vždy jen sociální síť, odkud zaměstnavatel získá informace, na základě kterých se rozhodne uchazeče o zaměstnání nepřijmout. Není výjimkou ani v České republice, že si společnosti vedou tzv. černé listiny (blacklisty) osob, které nechtějí zaměstnat. Problematika těchto blacklistů však souvisí s propuštěním zaměstnance, a proto je o ní blíže pojednáno až v následující kapitole.

Závěrem je snad ještě vhodné zmínit, co zaznělo v úvodu této podkapitoly, že ochrana soukromí zaměstnance má samozřejmě i určité limity. Shodně jako byla výše popsána ochrana osobnosti uchazeče o zaměstnání, má jistě svoji relevanci též právo zaměstnavatele na ochranu jeho majetku. V ustanovení § 30 odst. 1 ZPr[193] je přitom jasně potvrzeno právo zaměstnavatele provádět výběr uchazečů o zaměstnání. Stejně jako v jiných, v této práci popisovaných případech, také zde jde primárně o střet dvou práv, kterými jsou ochrana osobnosti zaměstnance a ochrana majetku zaměstnavatele (spočívající v nároku vybrat si „nejvhodnějšího“ uchazeče o zaměstnání). Zcela jednoznačně vymezit,

---

[191] Výjimkou je možnost získávat informace od předchozího zaměstnavatele, kde je dotázaný (bývalý) zaměstnavatel oprávněn podávat pouze ty informace, které jsou obsahem pracovního posudku, neudělí-li zaměstnanec souhlas s tím, že budou poskytnuty též jiné informace (srov. § 314 odst. 2 ZPr).

[192] Srov. výše uvedený výklad k finskému zákonu na ochranu soukromí v pracovním životě.

[193] Podle tohoto ustanovení platí, že „*výběr fyzických osob ucházejících se o zaměstnání z hlediska kvalifikace, nezbytných požadavků nebo zvláštních schopností je v působnosti zaměstnavatele, nevyplývá-li ze zvláštního právního předpisu jiný postup […]*“.

které informace může zaměstnavatel vyžadovat, není obecně možné. Vždy bude záležet na výsledku proporcionality posouzení těchto dvou práv. Pokud by se uchazeč o zaměstnání domníval, že zaměstnavatel toto vyhodnotil chybně a ptá se jej na něco, na co nemá nárok, případně by si o něm vyhledával pro zaměstnání nerelevantní informace, pravděpodobně by mezi nimi vznikl spor, který by musel rozhodovat soud.

4.2 Ochrana po skončení pracovního poměru

Ač by se mohlo zdát, že ochranu osobnosti je relevantní řešit pouze před vznikem pracovního poměru a v době jeho trvání, je takovýto závěr chybný. S výjimkou případů, kdy zaměstnanec odchází do penze, kdy se rozhodne dále podnikat nebo kdy z jiného důvodu přestane mít zájem o jakékoliv budoucí zaměstnání, má každý zájem najít si po skončení pracovního poměru co nejdříve zaměstnání nové. Aby k tomu došlo, je přitom důležité mít dobré hodnocení od zaměstnavatele původního. Takové hodnocení původního zaměstnavatele se přitom může projevovat zejména ve dvou rovinách, kterými jsou pracovní posudek a tzv. černé seznamy a o kterých je blíže pojednáno v této podkapitole.

4.2.1 Pracovní posudek

V souvislosti s ukončením pracovního poměru (nejdříve dva měsíce před jeho ukončením)[194] má zaměstnanec právo požádat, aby mu zaměstnavatel vydal posouzení pracovní činnosti, tzv. pracovní posudek. Zaměstnavatel je následně povinen mu jej vydat do 15 dnů od takové žádosti.[195] Podle věty druhé § 314 odst. 1 ZPr se pracovním posudkem rozumí *„veškeré písemnosti týkající se hodnocení práce zaměstnance, jeho kvalifikace, schopností a dalších skutečností, které mají vztah k výkonu práce“*. Ač zaměstnavatel není oprávněn v rámci posudku uvádět nic nad rámec výše uvedené definice, je z její textace zřejmé, že obsahově může být pracovní posudek velmi široký, jelikož vztah k výkonu práce může mít nejen výkonnost zaměstnance, jeho spolehlivost, pracovitost, ale i jeho vlastnosti a způsob jakým vychází s ostatními zaměstnanci.[196] Toto potvrdil též Nejvyšší soud ČR, když ve svém rozhodnutí vydaném pod sp. zn. 21 Cdo 2152/2004, ze dne 17. května 2005, uvedl mimo jiné: *„Pracovní posudek tedy může obsahovat i hodnocení celkového vztahu zaměstnance ke spolupracovníkům a k práci, jakož i hodnocení těch jeho osobních*

[194] Za zmínku stojí skutečnost, že zaměstnanec může požádat o vydání pracovního posudku rovněž po skončení pracovního poměru. Tento závěr byl potvrzen též judikaturou (srov. rozhodnutí Nejvyššího soudu ČR ze dne 22. dubna 2003, sp. zn. 21 Cdo 1893/2002).
[195] Srov. věta první § 314 odst. 1 ZPr.
[196] Fetter, R. W. *Pracovní posudek*. Právní rádce, 2010, č. 8, s. 21.

vlastností, které mají bezprostřední vztah k výkonu jeho práce, jako je svědomitost, iniciativnost, dodržování pracovní kázně, schopnost k řízení a organizování pracovního procesu, schopnost zapojit se do týmové práce s ostatními zaměstnanci apod.“.

S ohledem na výše uvedené, je snad nepochybné, že pracovní posudek může z hlediska svého obsahu představovat citelný zásah do ochrany osobnosti zaměstnance. Nejvyšší soud ČR proto ve výše uvedeném rozhodnutí rovněž vytyčil mantinely, za které by pracovní posudek neměl jít, když uvedl: *„Pracovní posudek se současně musí omezit na konkrétní hodnocení činnosti zaměstnance u bývalého zaměstnavatele a nemůže vyjadřovat v obecné rovině jeho subjektivní hodnotící názor (doporučení) na vhodnost budoucího působení zaměstnance v určitém okruhu pracovních činností.“*[197] Tento závěr je sice nepochybně správný, Putna však trefně poznamenává, že jeho splnění bude velmi obtížné, neboť *„již samotný požadavek, že pracovní posudek má obsahovat „hodnocení“, znamená, že bude vždy charakterizován vlastními (subjektivními) soudy hodnotitele (zaměstnavatele), zejména oněch dalších skutečností, práce zaměstnance a jeho schopností, jež mají vztah k vykonávané práci […]“.*[198]

Je proto realitou, že napsat objektivní pracovní posudek je velmi obtížné. Závažné to pak je v případě, kdy pracovní posudek vyznívá v neprospěch zaměstnance (resp. zaměstnanec s ním není spokojen), ačkoliv může nastat i opačná situace, kdy bude pracovní posudek nepravdivě pozitivní. V takové situaci však nedojde k žádné újmě v ochraně osobnosti zaměstnance, potenciálně bude hrozit uvedení v omyl budoucího zaměstnavatele, který bude z takového posudku vycházet. Pokud bude ale pracovní posudek pro zaměstnance negativní, může se zaměstnanci značně zkomplikovat hledání nového zaměstnání (například v situaci, kdy si zaměstnavatel vyžádá pracovní posudek od předchozího zaměstnavatele).

Z výše uvedených důvodů je zaměstnanci umožněno se vůči obsahu pracovního posudku bránit. Ustanovení § 315 ZPr dává zaměstnancům možnost se u soudu žalobou domáhat, aby bylo zaměstnavateli uloženo pracovní posudek přiměřeně upravit, a to do 3 měsíců, kdy se zaměstnanec o jeho obsahu dozvěděl. Ač se může zdát být takový proces zdlouhavý, není asi jiné lepší varianty, jak technicko-legislativně tento problém vyřešit, navíc o neobjektivnosti zaměstnavatelem vydaného pracovního posudku bude svědčit již soudní rozhodnutí, kterým bude uložena úprava posudku či vydání nového.

---

[197] Srov. rozhodnutí Nejvyššího soudu ČR ze dne 17. května 2005, sp. zn. 21 Cdo 2152/2004.
[198] Putna in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1234.

Pokud jde o otázku, kdy a za jakých podmínek bude zaměstnanci s jeho žalobou vyhověno, rozhodně neplatí, že by se zaměstnanec mohl svého požadavku domoci kdykoliv. Cílem je pouze dosažení pracovního posudku, který bude co možná nejvíce objektivní, nikoliv podle přání zaměstnance. Nejvyšší soud ČR v této souvislosti již judikoval ve svém rozhodnutí ze dne 18. července 2013, sp. zn. 21 Cdo 1362/2012, že *„přiměřenou úpravu posudku o pracovní činnosti lze požadovat jen v případě, je-li nesprávný, zejména ve vztahu k uváděným skutečnostem, k hodnocení činnosti zaměstnance vztahující se k výkonu jeho práce, anebo hodnotí-li skutečnosti, které nemají vztah k výkonu práce zaměstnance“*.[199] Pokud tedy toto nebude splněno, bude se zaměstnanec domáhat změny pracovního posudku bezúspěšně. Nicméně lze konstatovat, že právní úprava v tomto ohledu dostatečně zajišťuje, aby nebylo zasahováno do jeho práva na ochranu osobnosti nesprávným posudkem.

Závěrem tohoto bodu je vhodné ještě poznamenat, že pracovní posudek není potvrzením o zaměstnání. Potvrzení o zaměstnání je v ustanovení § 313 ZPr jasně definovaným dokumentem, který je zaměstnavatel povinen vydat a který má zákonem jasně definované obsahové náležitosti (údaje o zaměstnání a době jeho trvání, druh konaných prací, dosažená kvalifikace, odpracovaná doba a expozice, provádění srážek atd.).[200] S ohledem na to hrozí ve vztahu k potvrzení o zaměstnání nižší riziko zásahu do ochrany osobnosti zaměstnance, jelikož zaměstnavatel má jasně vymezeno, co má v potvrzení uvést, a v podstatě nemá možnost se od toho odchýlit. A kdyby snad k určitému odchýlení došlo, má zaměstnanec i v tomto případě v souladu s ustanovením § 315 ZPr právo domáhat se u soudu, aby zaměstnavatel potvrzení o zaměstnání přiměřeně upravil.

4.2.2 Černé seznamy (blacklisty)

Druhým faktorem majícím vliv na ochranu osobnosti zaměstnance po skončení pracovního poměru jsou tzv. černé seznamy, lépe známé pod anglickým označením blacklisty. I v tomto případě je důležité se jimi zabývat, jelikož mohou znamenat a mnohdy znamenají citelný zásah do možnosti zaměstnance ucházet se o novou práci u dalšího zaměstnavatele (nejde tedy již o vztah k zaměstnavateli, u nějž byl pracovní poměr ukončen). Zjednodušeně řečeno se jedná o vedení seznamu zaměstnanců, kteří jsou nepřijatelní pro další zaměstnání. Důvody zařazení na takový seznam přitom mohou být

[199] Rozhodnutí Nejvyššího soud ČR ze dne 18. července 2013, sp zn. 21 Cdo 1362/2012.
[200] Srov. ustanovení § 313 ZPr.

různé, může jít například o skutečnost, že daní zaměstnanci jsou nespolehliví, jsou potížisté, mají extrémní politické názory nebo jsou aktivní odboráři.[201]

Pokud je taková černá listina vedena výhradně na úrovni zaměstnavatele (tj. není s nikým sdílena) ve vztahu k osobám, které u něj byly dříve zaměstnány, a zaměstnavatel má pro vedení osoby na takové listině oprávněný důvod, pravděpodobně tomu nelze nic vytýkat. Co když ale bude taková černá listina sdílena mezi vícero společnostmi? V situaci, kdy bude taková listina následně využívána více zaměstnavateli v určité oblasti, kde uchazeč o zaměstnání žije, nebo mezi společnostmi v určitém odvětví, na které se uchazeč specializuje, může to mít pro zaměstnance naprosto fatální důsledky.

Takové praktiky, byť nejsou nikde oficiálně zaznamenány, nejsou zcela ojedinělé. Podíváme-li se na území Spojených států amerických, je písemně zachycena existence blacklistingu dokonce již od konce 18. století, kdy bývala v tehdejším měsíčníku pravidelně publikována jména zaměstnanců, kteří zpochybnili autority svých zaměstnavatelů.[202] V dřívější době byl blacklisting spojen především s účastí zaměstnanců v odborech či v politických stranách a hnutích. Je přitom zřejmé, že skutečnost, že se zaměstnanec objevil na blacklistu, měla nedozírné následky. Zaměstnanci často nebyli schopni najít práci ve svém oboru a nebylo ani výjimkou, že byli donuceni změnit si své identity nebo museli zcela opustit oblast, ve které žili.[203] Ve 20. století byl následně pojem blacklistingu spojen s érou McCarthyho, kdy docházelo k vytváření obvinění ze spojitosti s komunismem a provádění následných vyšetřování, což mělo za následek (ač se obvinění mnohdy nepotvrdila) ukončení zaměstnání a kariéry tisíců zaměstnanců.[204] Toto období dalo dokonce vzniknout dnes známému označení mccarthismus.

Že jde o problém, který se netýká ryze Spojených států amerických, je snad zřejmé. Důkazem je například více než třísetstránkový sborník vydaný v roce 2013 pod názvem „Blacklisting employees“ na půdě britského parlamentu, popisující desítky či stovky takovýchto praktik, ke kterým došlo na území Velké Británie.[205] Na území České republiky

---

[201] Vymětal, P. *Černé listiny* [online]. Pracovní text pro Ministerstvo vnitra ČR. Katedra politologie, Fakulta mezinárodních vztahů, Vysoká škola ekonomická v Praze, s. 1. [cit. 2019-02-10]. Dostupné z: https://www.mvcr.cz/soubor/studie-vymetal-blacklisting-pdf.aspx

[202] Weir, R. E. *Workers in America: a historical encyclopedia*. Vol. 1. Santa Barbara, California. ABC-CLIO, LLC, 2013, s. 71.

[203] Tamtéž.

[204] Steinbock, D. J. *Designating the Dangerous: From Blacklists to Watch Lists* [online]. Seattle University Law Review, Vol. 30:65, 2006, s. 65. [cit. 2019-02-05]. Dostupné z: https://ssrn.com/abstract=905299

[205] Sborník Dolní Komory Spojeného království: House of Commons, Scottish Affairs Committee. *Blacklisting in Employment. Oral and written evidence*. Publikováno 16. dubna 2013 [online]. [cit. 2019-02-10]. Dostupné z: https://publications.parliament.uk/pa/cm201213/cmselect/cmscotaf/156/156i.pdf

je však obtížnější hledat písemné zprávy a záznamy o tomto jevu.[206] Důvodem existence menšího počtu záznamů je podle názoru autora skutečnost, že se často o těchto seznamech veřejně nemluví.

Z výše uvedeného tedy vyplývá, že se jedná o velmi závažný problém s potenciálem mít fatální důsledky pro zaměstnance a že se s ním lze setkávat i na území České republiky. V návaznosti na to se nabízí několik otázek. Především, jak se proti takovému jednání může daný zaměstnanec bránit? Má šanci se nějak dozvědět, že takový seznam existuje a že je na něm evidován? Má právo na vysvětlení a právo bránit se proti chybně uvedeným informacím?

Pokud se budeme na tuto záležitost dívat z hlediska ochrany osobních údajů, odpověď na tyto otázky bude vesměs kladná.[207] Je toto ale dostatečné, přestože sankce za porušení pravidel ochrany osobních údajů jsou nepochybně velmi vysoké? Autor této práce se domnívá, že nikoliv, a to i přesto, že se na dané případy šíření informací bude aplikovat též ustanovení § 314 odst. 2 ZPr, které zaměstnavatelům zakazuje podávat o zaměstnancích jiné informace než ty, které mohou být obsahem pracovního posudku (neudělí-li zaměstnanec souhlas k poskytnutí i jiných informací). Tato ochrana je nedostatečná. Předně je zřejmé, že část informací je možné podle tohoto ustanovení šířit o zaměstnancích bez jejich přivolení. Navíc se tato ochrana týká jen podávání informací na žádost,[208] ačkoliv černé listiny jsou vytvářeny zaměstnavateli „preventivně“ pro budoucí využití, aniž by jakákoliv žádost o informace o zaměstnanci existovala. Nadto není nijak upraveno poskytnutí těchto informací pro jejich další systematizované zpracování, zejména tedy v rámci zmiňovaných blacklistů.

Ačkoliv by v tomto ohledu mohla být nápomocna regulace ochrany osobních údajů, příslušná ustanovení nařízení GDPR omezující možnost zpracovávat osobní údaje jen tehdy, svědčí-li pro to odpovídající právní základ (a tedy vysoká pravděpodobnost porušení těchto pravidel při vytváření černých listin), jsou pro daný problém až příliš obecná (vzdálená), nemluvě o skutečnosti, že dané černé listiny jsou obvykle utajované a není snadné se o jejich existenci dozvědět. Černá listina ani nemusí fyzicky existovat a být sdílena na úrovni více

[206] Určité zmínky však lze dohledat (srov. op. cit. sub. 201, s. 3 a násl.).
[207] S ohledem na právo na přístup k osobním údajům, srov. výklad v bodě 7.2.1.
[208] Srov. Putna in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1235.

společností, ale může se jednat o prosté vyměňování informací mezi personalisty. Pak ani pravidla na ochranu osobních údajů příliš nepomohou.

Podle autora této práce by danému problému nicméně pomohlo, pokud by existoval explicitní zákaz takových černých listin, a to v rámci ZPr či jiného obdobného předpisu. Samozřejmostí pro účelnost takového ustanovení by bylo, že by musela existovat jasně určená autorita (například úřad inspekce práce), která by na dodržování takového pravidla dohlížela, a musela by být jasně stanovena sankce za porušení tohoto pravidla. Aniž by to nějakým způsobem mohlo pomoci k odhalování existence takovýchto seznamů, mělo by to přinejmenším odstrašující efekt.

Taková právní úprava by přitom nebyla raritou. Příkladem obdobného pravidla může být trestní zákon státu Severní Karolina, kde existuje skutková podstata uvedení zaměstnance na černou listinu („blacklisting employees“). Podle této skutkové podstaty se za trestný čin považuje, zjednodušeně řečeno, pokud osoba či společnost po propuštění zaměstnance tomuto bývalému zaměstnanci zabrání nebo se pokusí zabránit získat zaměstnání u jiné osoby či společnosti.[209] Za spáchání takového trestného činu je přitom možné udělit citelnou finanční pokutu (až do výše 500 tisíc USD). Vedle toho nic samozřejmě nevylučuje uplatnění soukromoprávní žaloby na náhradu škody. Naopak je výslovně uvedeno, že trestným činem nebude, pokud si společnost, u které se hlásí nový uchazeč o zaměstnání, prověří historii uchazeče, včetně případných důvodů jeho propuštění, na svoji vlastní (písemnou) žádost. Nechť je tedy takováto norma inspirací též pro budoucí zákonodárce, neboť problém černých listin, ačkoliv se o něm příliš nemluví a nelze se o něm ani mnoho dočíst, se jistě týká též zaměstnanců v České republice a jde o závažný problém.

4.3 Ochrana osobnosti zaměstnance mimo výkon práce

Ochraně osobnosti „zaměstnaného“ zaměstnance během výkonu práce se věnuje celá následující kapitola 5. Předmětem této podkapitoly jsou tudíž pouze další aspekty ochrany osobnosti zaměstnance, které se na něj vztahují, i když práci pro svého zaměstnavatele právě nevykonává, nebo platí bez ohledu na to, zda ji vykonává či nikoliv. Jedná se především o ochranu osobnosti zaměstnance mimo pracovní dobu a dále o relativně samostatnou otázku osobního spisu zaměstnance.

---

[209] Kodex Severní Karoliny, Kapitola 14 Trestní právo. Článek 45 – Regulace zaměstnavatele a zaměstnance. 14-355. Blacklisting employees (cit. NC Gen Stat § 14-355) [online]. [cit. 2019-02-11]. Dostupný z: https://www.labor.nc.gov/workplace-rights/employee-rights-regarding-time-worked-and-wages-earned/job-reference-and-0

4.3.1 Soukromý život zaměstnance

Do jaké míry může zaměstnavatel zasahovat do soukromého života zaměstnance ve smyslu toho, co zaměstnanec dělá mimo pracovní dobu? Může například sledovat zaměstnancovo chování na internetu, na veřejnosti, může sledovat jeho pohyb? Může ze zjištěných skutečností vyvozovat nějaké důsledky pro zaměstnance? Předmětem této podkapitoly je uvedené otázky analyzovat a nalézt na ně odpovědi. Avšak pouze v rozsahu daném tím, že zaměstnanec v rámci svého soukromého života nevyužívá žádné prostředky svěřené mu ze strany zaměstnavatele. Pokud jde o zaměstnavatelem svěřené prostředky a možnost využití zvláštních monitorovacích zařízení, umožňujících sledování využívání svěřeného telefonu nebo počítače pro soukromé účely, nebo sledování služebních vozidel pomocí GPS při soukromých cestách, věnuje se těmto otázkám blíže podkapitola 8.1.

Před vlastní analýzou možných střetů zaměstnancova soukromého života s právy a zájmy zaměstnavatele je ještě nutné se zamyslet nad otázkou loajality zaměstnance vůči zaměstnavateli. Podle ustanovení § 301 písm. d) ZPr jsou zaměstnanci povinni *„řádně hospodařit s prostředky svěřenými jim zaměstnavatelem a střežit a ochraňovat majetek zaměstnavatele před poškozením, ztrátou, zničením a zneužitím a nejednat v rozporu s oprávněnými zájmy zaměstnavatele“*. Zejména pak povinnost nejednat v rozporu s oprávněnými zájmy zaměstnavatele[210] má hlubší rozměr a lze z ní dovozovat povinnost loajality zaměstnance vůči zaměstnavateli.[211] Povinnost loajality zaměstnance má přitom historickou tradici a je úzce spjata se samotnou podstatou vztahu mezi zaměstnancem a zaměstnavatelem. To potvrzuje též judikatura ESLP, když tento soud mimo jiné dovozuje zaměstnancovu povinnost loajality, mlčenlivosti a zdrženlivosti.[212] Pokud jde o právo na svobodu projevu, ESLP také dovodil, že rozsah práva na svobodu projevu, který by byl obecně přijatelný v jiných podmínkách, nemusí být přijatelný v podmínkách vztahu zaměstnance a zaměstnavatele.[213] Ve stejném smyslu si povinnosti loajality všímá též česká judikatura.[214] Zvláštní kategorií je následně loajalita státních zaměstnanců, respektive

[210] Obdobně též ustanovení § 1a odst. 1 písm. d) ZPr.
[211] Shodně srov. Bělina in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1170.
[212] Srov. například rozhodnutí ESLP ze dne 13. ledna 2015 ve věci Rubins vs. Lotyšsko, č. stížnosti 79040/12.
[213] Tamtéž.
[214] Srov. například rozhodnutí Nejvyššího soudu ČR ze dne 21. ledna 2014, sp. zn. 21 Cdo 1496/2013, ve kterém soud zdůraznil, že „*ve vztazích zaměstnavatele a zaměstnance je nezbytná vzájemná důvěra, spolehlivost zaměstnance a jeho poctivost ve smyslu § 301 písm. d) zákoníku práce. Zákon zároveň ukládá zaměstnanci, aby celým svým chováním v souvislosti s pracovním vztahem nezpůsoboval zaměstnavateli škodu, ať už majetkovou nebo morální.“*.

zaměstnanců ve služebním poměru, ale bližší popis této otázky již překračuje potřeby této práce.

Pokud jde o možnost monitorování zaměstnancova soukromého majetku, jako je například využívání jeho soukromého PC, mobilu či automobilu, ze strany zaměstnavatele, v podstatě neexistuje legální možnost, jak by se k těmto informacím zaměstnavatel mohl dostat.[215] A pokud se k nim dostane, závažnější než porušení ochrany osobnosti, ke kterému nepochybně také dojde, bude trestněprávní aspekt takového zaměstnavatelova jednání. Proto není záměrem se těmito otázkami blíže zabývat. Naopak předmětem zkoumání v této podkapitole je tudíž využití informací o zaměstnancově soukromém životě, u kterých je reálné, že se k nim zaměstnavatel dostane, aniž by přitom vyloženě páchal trestný čin. Půjde například o získání komunikace s jinými osobami, včetně jiných zaměstnanců, zaměstnancem dobrovolně a vědomě sdílené výroky na veřejnosti či na sociálních sítích či doklad o jakémkoliv jiném jednání zaměstnance, které má (nebo alespoň v očích zaměstnavatele může mít) souvislost s jeho pracovněprávním vztahem u daného zaměstnavatele.

Je patrné, že v těchto případech mnohdy nejde jen o otázku ochrany osobnosti. Důležité je rovněž zkoumat svobodu projevu zaměstnance. Naproti tomu u zaměstnavatele nejde vždy jen o ochranu jeho majetku, ale mnohdy též o ochranu jeho dobré pověsti (ač ta je s ochranou majetku nepřímo provázána). Nicméně nebude tomu tak vždy a tyto případy je nutné důsledně rozlišovat. Pokud totiž zaměstnanec sám určité své výroky či jiné jednání učiní veřejně přístupnými, jen stěží může očekávat, že takové výroky či jednání budou podléhat ochraně jeho soukromí. Na druhou stranu v situacích, kdy výrok či jiné jednání budou učiněny v omezeném okruhu osob, s úmyslem, aby se dále nešířily, je relevantní se ochranou osobnosti a soukromí zaměstnance zabývat.

Situace, kdy zaměstnanci sami zveřejní informace, ke kterým se následně dostane zaměstnavatel (a ten z nich vyvodí určité důsledky), jsou poměrně časté. Jak bylo naznačeno, obvykle v těchto sporech nejde o ochranu osobnosti zaměstnanců, nýbrž především o střet práva na ochranu svobody projevu zaměstnance s právem zaměstnavatele na ochranu dobré pověsti. Jedná se tedy o situace, kdy se zaměstnancovo jednání či výrok dotýkají

---

[215] Výjimkou mohou tvořit určité mezní situace, kdy existuje vyšší zájem na sledování, který převáží ochranu soukromí zaměstnance. Například jde o sledování vychovatele, který má pedofilní sklony, investičního bankéře, který je gambler či podobné extrémy (blíže viz Vidrna, J., Koudelka, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců*. V Praze: C.H. Beck, 2013. Beckova edice ABC, s. 205 a násl.).

zaměstnavatele, ba dokonce jej přímo poškozují. Čas od času se stávají tyto situace předmětem sporu, který je řešen až u Nejvyššího soudu ČR či Ústavního soudu ČR. Příkladem je zejména rozhodnutí Nejvyššího soudu ČR ze dne 20. března 2017, sp. zn. 21 Cdo 1043/2016, ve kterém se soud zabýval oprávněností okamžitého zrušení pracovního poměru se zaměstnancem, který se jako novinář na internetovém zpravodajském serveru veřejně vyjádřil poškozujícím způsobem o svém zaměstnavateli (v podstatě uvedl, že u zaměstnavatele dochází k neúměrnému zasahování do zpravodajských reportáží a tím k cenzuře).

Soud se v daném případě zcela správně věnoval pouze otázce loajality zaměstnance vůči zaměstnavateli, svobody projevu zaměstnance a otázce dobré pověsti zaměstnavatele. Dospěl přitom k závěru, že okamžité zrušení pracovního poměru bylo v daném případě namístě, neboť svoboda projevu není neomezená a *„může dojít k zásahu do práva na zachování dobré pověsti fyzické nebo právnické osoby nejen zveřejněním nepravdivých (nepodložených) znevažujících (difamujících) skutkových tvrzení, která jsou objektivně způsobilá ohrozit či poškodit dobrou pověst dotčené osoby, ale i zveřejněním nepřípustných hodnotících úsudků o určité osobě“.*[216] Kritiku soud připustil, jen pokud by šlo o přípustnou či oprávněnou kritiku, která by byla *„věcná a konkrétní a současně přiměřená co do obsahu, formy i místa, tj. že nevybočuje z mezí nutných k dosažení sledovaného a zároveň uznaného cíle (tedy – řečeno jinak nesmí být vzhledem k cílům kritiky přemrštěná, přehnaná). Věcnost kritiky vyžaduje, aby vycházela z pravdivých (podložených) skutkových tvrzení […].“.*[217] O žádném zásahu do ochrany osobnosti tedy v tomto případě nebyla řeč.[218]

Co ale v již naznačeném případě, kdy výrok či jiné jednání zaměstnance budou učiněny v omezeném okruhu osob nebo za jiných podmínek, kdy bude jasný zaměstnancův úmysl, aby se daný výrok či jiné jednání dále nešířily, zejména ne k zaměstnavateli? Nechme teď stranou otázku toho, zda se bude jednat o oprávněnou či neoprávněnou kritiku

---

[216] Rozhodnutí Nejvyššího soudu ČR ze dne 20. března 2017, sp. zn. 21 Cdo 1043/2016.
[217] Tamtéž. Oprávněnou kritiku přitom soudy připustily již dříve, srov. rozhodnutí Nejvyššího soudu ČR ze dne 21. března 2013, sp. zn. 21 Cdo 560/2012, nebo nález Ústavního soudu ČR ze dne 15. března 2005, sp. zn. I. ÚS 367/03.
[218] Obdobně nebude možné hledat zásah do ochrany osobnosti v případě zaměstnance, který svou kritiku sdělí přímo svému zaměstnavateli (a ten ji následně použije proti zaměstnanci). I takovýto spor byl řešen českými soudy, konkrétně šlo o případ, kdy se zaměstnanec vyjádřil kriticky o fungování svého zaměstnavatele v rámci interní porady. I v tomto případě byl pracovní poměr zaměstnance okamžitě zrušen, avšak v tomto případě došlo k zneplatnění tohoto okamžitého zrušení s odkazem na to, že v dané situaci zaměstnanec pouze (interně) pronesl kritické hodnotové soudy či stanoviska, jimiž měl v úmyslu zejména upozornit na některé nedostatky v činnosti a hospodaření zaměstnavatele (srov. nález Ústavního soudu ČR ze dne 23. března 2010, sp. zn. I. ÚS 1990/08).

zaměstnavatele ve smyslu výše uvedených rozhodnutí Nejvyššího soudu ČR nebo zda půjde o výrok či jednání, které jej mohou poškozovat (a předpokládejme, že ano). Hledisko svobody projevu zaměstnance bude v tomto případě v podstatě bezpředmětné. Naopak bude důležité zkoumat, zda nedošlo k porušení ochrany osobnosti zaměstnance spočívající v narušení jeho soukromí. Pokud jde o otázku loajality zaměstnance, ta může (ale nemusí) být v posuzovaném případě relevantní. Bude záviset na tom, do jaké míry zaměstnanec svým jednáním poruší výše zmíněné prvky, definované judikaturou ESLP, a poruší svou loajálnost, zdrženlivost či mlčenlivost, čímž dojde k porušení oprávněných zájmů zaměstnavatele.[219]

Ani pokud by došlo k porušení loajálnosti zaměstnance vůči jeho zaměstnavateli, z čehož by mohlo být vyvozováno porušení ochrany dobré pověsti zaměstnavatele nebo porušení ochrany jeho majetku, nemusí být podle názoru autora této práce vždy takové zjištění vůči zaměstnanci použitelné, a to právě z toho důvodu, že by tím došlo k zásahu do ochrany osobnosti zaměstnance. Samozřejmě vždy bude záležet na konkrétních skutkových okolnostech případu, zejména na tom, jaká bude povaha jednání zaměstnance a jakým způsobem se zaměstnavatel k informacím dostane. Z judikatury ESLP je nicméně zřejmé, jak široce je v poslední době nahlíženo na legitimní očekávání soukromí zaměstnance.[220] Vzhledem k tomu, že ESLP tuto ochranu široce dovozuje a přiznává zaměstnanci při výkonu jeho práce, o to spíše by pak měla být dovozována v soukromém životě zaměstnance, tj. mimo pracovní dobu.

Určitou paralelu podporující tento závěr lze vést též s odkazem na nález Ústavního soudu ČR sp. zn. II. ÚS 1774/14, ze dne 9. prosince 2014. V tomto případě šlo skutkově o to, že zaměstnanec napadal ukončení svého pracovního poměru pro nadbytečnost tím, že se o nadbytečnost nejednalo, nýbrž byl pracovní poměr ukončen z důvodu, že kritizoval svého zaměstnavatele. Tuto skutečnost přitom zaměstnanec dokládal tajně pořízenou nahrávkou z rozhovoru s členem zahraničního vedení zaměstnavatele. V dané situaci přitom Ústavní soud testem proporcionality poměřoval, zda „*má převážit zájem na ochraně práv stěžovatele, který si uvedenou audionahrávku pořídil a následně použil jako důkaz v řízení před obecnými soudy, a to za účelem prokázání svých tvrzení o skutečném důvodu výpovědi z pracovního poměru, případně, zda je důležitější zájem na ochraně osobnosti nahrávaného*

[219] Srov. ustanovení § 301 odst. 1 písm. d) ZPr.
[220] Srov. kapitola 3.3.

člena zahraničního vedení“.[221] Soud nakonec rozhodl ve prospěch zaměstnance a zásah do ochrany osobnosti nahrané osoby neuznal.

Kromě té skutečnosti, že na pořízené nahrávce nebyly žádné informace osobní povahy, zdůraznil soud rovněž skutečnost, že *„za běžných okolností je svévolné nahrávání soukromých rozhovorů bez vědomí jejich účastníků hrubým zásahem do jejich soukromí. Takovýto postup s rysy záludnosti je ve velké většině případů morálně i právně zcela nepřijatelný […]. Zcela odlišně je však třeba posuzovat případy, […] jde-li o způsob dosažení právní ochrany pro výrazně slabší stranu významného občanskoprávního a zejména pracovněprávního sporu. Zásah do práva na soukromí osoby, jejíž mluvený projev je zaznamenán, je zde plně ospravedlnitelný zájmem na ochraně slabší strany právního vztahu, jíž hrozí závažná újma (včetně např. ztráty zaměstnání).“.*[222]

Výkladem a contrario lze podle názoru autora této práce následně tyto závěry aplikovat na případy, kdy se zaměstnavatel dostane k informacím o výrocích či jednáních zasahujících nepřiměřeně do soukromí zaměstnance. V takové situaci se na rozdíl od případu posuzovaném Ústavním soudem ČR aplikuje ochrana ve prospěch slabší strany, tj. ve prospěch zaměstnance, do jehož práva na ochranu osobnosti bylo zasaženo. Naopak shodně bude vykládáno pravidlo o obecném zákazu zasahování do soukromí jednotlivce. Toto ve vzájemném propojení jen umocňuje závažnost zásahu do ochrany osobnosti zaměstnance. Samozřejmě můžou nastat skutkové okolnosti, které využití těchto informací zaměstnavateli umožní, půjde však obvykle o situace, kdy nebude jasně možné určit, zda zaměstnancovo jednání či výrok byly učiněny soukromě, nebo veřejně, a kdy zásah do soukromí zaměstnance nebude citelný. Toto bylo již posuzováno a potvrzeno Nejvyšší soudem ČR v rozhodnutí ze dne 4. dubna 2017, sp. zn. 21 Cdo 3998/2016, kdy soud shledal za přiměřené, že zaměstnavatel pořídil výpis telefonních hovorů zaměstnance (aniž by znal jejich obsah) a vyvodil z nich důsledky spočívající v ukončení pracovního poměru. Hranice však v některých případech může být neostrá.

4.3.2 Osobní spis zaměstnance

Dle ustanovení § 312 odst. 1 ZPr je oprávněním každého zaměstnavatele vést si o každém zaměstnanci osobní spis. Nabízí se však otázka, zda se nejedná spíše o povinnost, když zaměstnavatel musí plnit své povinnosti vyplývající mimo jiné ze ZPr a ZoZ, musí mít

[221] Nález Ústavního soudu ČR ze dne 9. prosince 2014, sp. zn. II. ÚS 1774/14.
[222] Tamtéž.

k dispozici pracovní smlouvu zaměstnance, doklady o kvalifikaci zaměstnance, podklady k prováděným srážkám ze mzdy, po skončení pracovního poměru rovněž dokumenty ohledně takového ukončení, ať už půjde o výpověď, dohody, okamžité zrušení apod. Vedle toho může mít mnoho dalších dokumentů, jako je osobní dotazník, platový výměr, podepsaná prohlášení zaměstnance (o BOZP, o seznámení se s pracovním řádem či s informací o nakládání s osobními údaji), souhlasy se zpracováním osobních údajů udělené zaměstnancem, vyjádření lékaře k pracovní způsobilosti, dohodu o odpovědnosti apod. Na základě toho lze uzavřít, že vést osobní spis zaměstnance je spíše povinnost než oprávnění zaměstnavatele. Použití spojení *„je oprávněn“* v rámci § 312 odst. 1 ZPr je však možné rozumět také tak, že zákonodárce chtěl dát zaměstnavateli jasný právní základ pro zpracování příslušných osobních údajů.

Pokud jde o účel vedení osobního spisu, je zřejmé, že jeho vedením dochází k naplňování pracovněprávní agendy. Nepochybně také přispívá k usnadnění práce vedoucích zaměstnanců při plnění jejich pracovních povinností, případně při kontrole plnění pracovních úkolů dotčeného zaměstnance.[223] Podle věty druhé ustanovení § 312 odst. 1 ZPr smí osobní spis *„obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu uvedeném v § 3“*. V předchozím odstavci bylo přitom naznačeno, o jaké písemnosti se bude obvykle jednat. Úplný výčet nicméně nelze poskytnout a rozhodně neplatí, že by osobní spisy dvou zaměstnanců měly a musely být totožné, a to i když jde o kolegy pracující na stejné pozici u téhož zaměstnavatele.[224] Za zmínku snad jen stojí, že nepochybně bude možné určit též dokumenty či informace, které obsahem osobního spisu být nemohou. Půjde zejména o informace a dokumenty odpovídající zákazu uvedenému v ustanovení § 316 odst. 4 ZPr či údaje, které zaměstnavatel nesmí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru ve smyslu ustanovení § 30 odst. 2 ZPr.[225] V opačném případě by došlo k zásahu do práva na ochranu osobnosti zaměstnance se všemi z toho vyplývajícími důsledky.

Z hlediska ochrany osobnosti lze v souvislosti s vedením osobního spisu kromě výše uvedeného identifikovat ještě jeden aspekt, a to otázku, kdo, kdy a za jakých podmínek má

---

[223] Morávek, J. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013, s. 394. Blíže k vedení osobního spisu též Mates, P., Janečková, E., Bartík, V. *Ochrana osobních údajů*. Praha: Leges, 2012, s. 82 a násl.

[224] K praktickým otázkám ohledně obsahu osobního spisu viz Bartík, V., Janečková, E. *Ochrana osobních údajů v aplikační praxi: vybrané problémy*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016, s. 141 a násl.

[225] Blíže viz bodě v kapitole 4.1.2.

přístup k osobnímu spisu zaměstnance. Rozhodně přitom platí, že k informacím o zaměstnanci by se měly dostat vždy jen osoby oprávněné, které takové informace potřebují pro výkon své práce a jsou zavázány odpovídající mlčenlivostí. Zákoník práce možnost nahlížet do osobního spisu upravuje v ustanovení § 312 odst. 2 ZPr,[226] v rámci kterého vypočítává osoby, které mají právo nahlížet do osobního spisu zaměstnance. Samozřejmostí je přístup vedoucích zaměstnanců příslušného zaměstnance a zaměstnance samotného.[227] Dále se jedná o přístup třetích osob (soudy, státní orgány a instituce), které budou obvykle u zaměstnavatele do spisu nahlížet v rámci výkonu své pravomoci. Putna[228] správně poznamenává, že výčet uvedený v tomto ustanovení není taxativní a přístup budou muset mít další osoby, kterými jsou například zaměstnanec vedoucí osobní spis, firemní právník, ředitel, případně statutární orgán zaměstnavatele apod.

Pro ochranu osobnosti zaměstnance bude mít klíčový význam přístup ostatních zaměstnanců a nadřízených (ze strany zmiňovaných třetích osob vyjmenovaných v ustanovení § 312 odst. 2 ZPr bude riziko zneužitelnosti informací podstatně nižší). Právě u takovýchto osob bude nutné dbát, aby byly zajištěny výše zmíněné podmínky na omezení přístupu a zachování mlčenlivosti. Zejména by přitom nemělo dojít ke zpřístupnění osobních údajů neoprávněné osobě, avšak i osoby oprávněné by k osobnímu spisu měly přistupovat jen v nutných případech a o takovém přístupu by měl být veden záznam. Ač mnohdy bude přístup těchto osob legitimní, je nutné brát na zřetel, že přistupují k potenciálně citlivým informacím, které mohou být snadno proti zaměstnanci zneužitelné. Přestože zákon zaměstnavateli říká, jaké údaje po zaměstnancích nemůže chtít a jaké nemůže zpracovávat,[229] zneužitelná může být v podstatě jakákoliv informace ve spise uvedená. Příkladem může být výše odměny zaměstnance (na jejímž utajení má mimo jiné zájem i sám zaměstnavatel). Rizikem jsou pak především zaměstnanci, kteří nejsou dotčenému zaměstnanci přímo nadřízení.

---

[226] Podle ustanovení § 312 odst. 2 ZPr platí: *„Do osobního spisu mohou nahlížet vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni. Právo nahlížet do osobního spisu má orgán inspekce práce, Úřad práce České republiky, Úřad pro ochranu osobních údajů, soud, státní zástupce, policejní orgán, Národní bezpečnostní úřad a zpravodajské služby. Za nahlížení do osobního spisu se nepovažuje předložení jednotlivé písemnosti zaměstnavatelem z tohoto spisu vnějšímu kontrolnímu orgánu, který provádí kontrolu u zaměstnavatele a který si tuto písemnost vyžádal v souvislosti s předmětem kontroly prováděné u zaměstnavatele.“*

[227] Přístup zaměstnance samotného je explicitně umožněn ustanovením § 312 odst. 3 ZPr. Tato úprava je však dnes v podstatě nadbytečná s ohledem na existenci práva zaměstnance na přístup k osobním údajům ve smyslu čl. 15 nařízení GDPR.

[228] Putna in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1226.

[229] Srov. výše uvedený výklad k obsahu osobního spisu zaměstnance.

5 Ochrana osobnosti zaměstnance při výkonu práce

Předmětem této kapitoly je detailní analýza kontrolních oprávnění zaměstnavatele vůči zaměstnancům ve střetu s jejich právem na ochranu osobnosti, jež zahrnuje zejména právo na soukromí, a to při výkonu práce.[230] S ohledem na to, že v daném případě dochází ke střetu dvou či více ústavou zaručených práv, jsou blíže popsány meze a limity těchto práv, a to jak ve vztahu k právům a povinnostem zaměstnanců, tak i ve vztahu k právům a povinnostem zaměstnavatelů. Analýza je prováděna v obecné rovině, přičemž analýza vybraných kontrolních mechanismů a opatření pro specifické případy (dopisy, e-maily, kamery, GPS, biometrie apod.) je poskytnuta v samostatné podkapitole 8.1. Předmětem dále není zkoumání povinností zaměstnavatele vyplývajících z ochrany osobních údajů, neboť tyto otázky jsou zkoumány samostatně v části III této práce. Zároveň je napříč kapitolou poskytováno autorovo hodnocení fungování platné právní úpravy, jejího výkladu obecnými soudy či ze strany odborné veřejnosti.

Jak bylo naznačeno, tato kapitola se zaobírá především kontrolními oprávněními zaměstnavatele vůči zaměstnancům. O skutečnosti, že zaměstnavatel nebo vedoucí zaměstnanci jsou oprávněni provádět kontrolu podřízených zaměstnanců, nikdo nepochybuje.[231] Platná právní úprava obsažená v rámci ZPr vymezuje několik situací, kdy a jak může zaměstnavatel své zaměstnance kontrolovat. S ohledem na slabší postavení zaměstnanců cílí příslušná ustanovení především na jejich ochranu. Aby se daná ustanovení nemíjela účinkem, rozhodl proto zákonodárce, že jsou všechna kogentní, resp. alespoň jednostranně kogentní (tj. umožňující odchýlení ve prospěch zaměstnance).[232] V následujících podkapitolách jsou nejprve postupně popsána tři základní kontrolní oprávnění související s ochranou osobnosti a soukromím zaměstnance. ZPr přitom zná i další kontrolní oprávnění zaměstnavatele (například týkající se BOZP), ta jsou však pro tento okamžik ponechána stranou, neboť míří primárně na ochranu jiného statku a mohou se překrývat (a mnohdy překrývají) s kontrolními oprávněními týkajícími se ochrany osobnosti.

---

[230] Přestože ochraně osobnosti v době, kdy zaměstnanec nevykonává práci, se věnovala též předchozí podkapitola 4.3, platí, že mnoho kontrolních mechanismů popisovaných v této kapitole bývá uplatňováno ze strany zaměstnavatele během výkonu práce i mimo něj.

[231] Srov. například ustanovení § 11 ZPr či § 302 písm. a) ZPr.

[232] Srov. ustanovení § 4a ZPr.

5.1 Kontrola vnášených věcí

Je přirozené, že zaměstnanci si s sebou berou na pracoviště též své osobní věci. Mnohdy přitom nejde o věci, které by zaměstnanci nutně potřebovali pro výkon práce. Pokud odhlédneme od věcí osobní potřeby a nutné spotřeby, jako je oblečení zaměstnance a strava, půjde zejména o různé šperky a jiné cennosti, mobilní telefony, hodinky a jiná podobná zařízení. Může jít ale i o věci, které zaměstnanec ani s sebou ani běžně nenosí, ani mu nepatří, jen je například potřebuje na pracovišti uložit do doby svého odchodu. Samozřejmostí je, že si pak chtějí tyto své věci opět odnést. Vnášení určitých předmětů však nemusí být vždy z nejrůznějších důvodů vhodné, například protože jsou dané předměty nebezpečné, na pracovišti nevhodné nebo by mohly zaměstnavateli způsobit škodu. Vedle toho není ani pochyb o tom, že by si zaměstnanec neměl nikdy odnést více, než co do zaměstnání přinesl. Zaměstnanec tedy nesmí nic zaměstnavateli (ani jiným zaměstnancům) odcizit.

Je proto srozumitelné, že zaměstnavatel má oprávnění toto do určité míry kontrolovat. Aby nicméně ze svého silnějšího postavení nezasahoval nadměrně do práv zaměstnanců a nedopouštěl se jejich nadměrného sledování, upravil zákonodárce limity tohoto zaměstnavatelova oprávnění v rámci ustanovení § 248 odst. 2 ZPr. Podle tohoto ustanovení platí, že zaměstnavatel je *„z důvodu ochrany majetku oprávněn v nezbytném rozsahu provádět kontrolu věcí, které zaměstnanci k němu vnášejí nebo od něho odnášejí, popřípadě provádět prohlídky zaměstnanců. Při kontrole a prohlídce podle věty první musí být dodržena ochrana osobnosti. Osobní prohlídku může provádět pouze fyzická osoba stejného pohlaví.“*.

Ačkoliv není citované ustanovení tolik diskutováno, předmětem sporů a vykládáno judikaturou jako dále probírané ustanovení § 316 ZPr, rozhodně je také důležité a je potřebné definovat kdy a za jakých podmínek může zaměstnavatel tyto kontroly provádět. Jako důvod, proč zaměstnavatel může provádět kontroly, je stanovena ochrana majetku zaměstnavatele. Ač se jedná o relativně široce definovaný účel, neboť ochrana majetku je pojmem, pod který bude možné za určitých okolností zahrnout téměř cokoliv, co náleží zaměstnavateli a s čím zaměstnanec přichází do styku, lze dojít k závěru, že by těžko bylo možné zaměstnavatelův zájem lépe definovat. Jakýkoliv jiný termín či chráněný zájem na straně zaměstnavatele by mohl být nadmíru restriktivní. Naopak je z uvedeného ustanovení jasné, že dané kontroly nemohou sledovat žádný jiný účel (například ověřování důvěryhodnosti a bonity zaměstnance).

Pokud jde o rozsah či limity provádění kontrol, používá ustanovení § 248 odst. 2 ZPr spojení „*v nezbytném rozsahu*“.[233] Z tohoto spojení je patrné, že zaměstnavatel při daných kontrolách není oprávněn postupovat svévolně a musí jednat co nejšetrněji, zejména ve vztahu k ochraně osobnosti zaměstnanců. Konkrétní míra toho, co si zaměstnavatel může dovolit, se však bude nepochybně lišit v závislosti na vykonávané práci. Je zřejmé, že kontroly ve větším rozsahu a množství budou obhajitelné v situacích, kdy zaměstnanci přicházejí do styku s předměty, které lze snadno odcizit (obchod, sklad), než v situacích, kde tato možnost obecně není (kancelář). Zároveň by mělo platit, že důkladnější prohlídku bude vždy možné provést jen při konkrétním podezření na odcizení věci.[234]

Pokud jde o provádění prohlídek, v praxi není pochyb o tom, že mohou být prováděny vedle zaměstnavatele též ze strany bezpečnostní agentury, [235] kterou k tomu zaměstnavatel zmocní a zaváže ji k dodržování povinností, jež budou v souladu s pravidly stanovenými v zákoně, případně v interních předpisech zaměstnavatele, které budou zákonné povinnosti blíže rozvádět. Při provádění kontrol nicméně musí být dodrženo zaměstnancovo právo na ochranu osobnosti, včetně toho, že osobní prohlídka bude prováděna osobou stejného pohlaví. V té souvislosti lze jen doporučit, aby byly bližší povinnosti stanoveny v interních předpisech zaměstnavatele. Pak by bylo totiž pro zaměstnance snazší domáhat se svých práv při případných porušeních takových pravidel, a naopak zaměstnavatel by snáze mohl prokazovat, že postupuje v souladu se zákonem a respektuje ochranu osobnosti svých zaměstnanců.[236]

Pokud by výše stanovené povinnosti dodrženy nebyly, měl by zaměstnanec možnost domáhat se ochrany ve smyslu příslušných ustanovení ObčZ. V dané situaci kontrol prováděných ze strany zaměstnavatele půjde zejména o možnost domáhat se toho, aby bylo od zásahu do jeho práva (tj. od daných kontrol) upuštěno. Do úvahy mohou připadat i jiné způsoby kompenzace, jako je například náhrada nemajetkové újmy. I přesto samozřejmě

---

[233] Za zmínku stojí skutečnost, že v průběhu roku 2016 byl projednáván návrh změny ZPr, na základě kterého mělo dotčené ustanovení znít: „*Je-li dán závažný důvod spočívající v povaze činnosti zaměstnavatele, je zaměstnavatel oprávněn k ochraně majetku v nezbytném rozsahu provádět […]*“, tj. mělo dojít k sladění s ustanovením § 316 odst. 2 Zpr. (srov. Landwehrmann, T. *Kontrola vnášených a vynášených věcí na pracovišti*. Praktická personalistika. 2016, č. 7-8., s. 19). K přijetí tohoto návrhu však nikdy naštěstí nedošlo, v opačném případě by totiž podle názoru autora této práce došlo k nadměrnému zásahu do práva na ochranu majetku zaměstnavatele.

[234] Landwehrmann, T. *Kontrola vnášených a vynášených věcí na pracovišti*. Praktická personalistika. 2016, č. 7-8., s. 20.

[235] Novotný in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1018.

[236] Jak bylo naznačeno výše, bližší pravidla pro provádění prohlídek by zaměstnavatel měl v každém případě určit, pokud k jejich výkonu využívá třetí osobu, zejména bezpečnostní agentury.

zůstává vztah mezi zaměstnancem a zaměstnavatelem vztahem pracovněprávním se všemi jeho specifiky.[237] Bohužel však, i přes tuto skutečnost, je význam tohoto ustanovení poněkud oslaben, jelikož jeho porušení není považováno za správní delikt. To považuje autor této práce za velký nedostatek.[238] Zaměstnanec, aby se domohl svého práva, se bude muset sám obrátit přímo na zaměstnavatele s následně obvykle na soud. To přirozeně samo o sobě vyvolá určité narušení vztahu mezi zaměstnancem a zaměstnavatelem. Rovněž lze vést určité pochybnosti o efektivitě a rychlosti, která je takovouto ochranou poskytována. Vše by přitom bylo možné snadno odstranit, pokud by existovala konkrétní sankce za porušení těchto pravidel.

Závěrem lze s ohledem na časté využívání kamerových systémů na pracovištích poznamenat, že jejich využití pro účely provádění kontrol ve smyslu § 248 odst. 2 ZPr se jeví jako spíše nevhodné. Komplexně je však o využití kamer na pracovišti pojednáno v bodě 8.1.5.

5.1.1 Zákaz vnášení předmětů

S problematikou provádění kontrol vnášených a odnášených předmětů také úzce souvisí otázka, do jaké míry může zaměstnavatel zaměstnancům zakázat na pracoviště vnášet či na něm umisťovat určité osobní předměty. To není pouhá teorie, ale denní realita například v rámci velkých skladových hal, kde se zaměstnavatelé snaží svým zaměstnancům zabránit v jakémkoliv odcizení uskladněných předmětů. Může jít nicméně též o restaurace, hotely, výrobní linky nebo jednoduše o kanceláře a zákaznické přepážky, na kterých přicházejí příslušní zaměstnanci do přímého styku se zákazníky a kde zaměstnavatelé zakazují zaměstnancům umisťovat osobní předměty s ohledem na snahu zaměstnavatele o vybudování určitého zákaznického „image“ společnosti.

Lze shrnout, že zaměstnavatelé těmito kroky sledují obvykle tři cíle. Jedním je ochrana jejich majetku, druhým je bezpečnost na pracovišti a třetím je vzhled pracoviště. Všechny tyto cíle jsou nepochybně do určité míry legitimní, ale mají též své limity, které vymezuje právo zaměstnanců na ochranu jejich osobnosti. Pro všechny dále uvedené případy, kdy zaměstnavatel sleduje zmíněné cíle, lze jednoznačně doporučit, aby

[237] Tamtéž.

[238] Zejména je pak škoda, že sankce za porušení této povinnosti nebyla zakotvena v rámci novely ZPr provedené zákonem č. 251/2005 Sb., kterým se změnil zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a dalšími souvisejícími zákony, jíž došlo mimo jiné k zavedení tolik chybějící sankce za porušení ustanovení § 316 ZPr.

zaměstnavatel jasně zakotvil zákaz vnášení do svého vnitřního předpisu a tento zákaz náležitě odůvodnil (pokud bude sledovaným cílem bezpečnost na pracovišti, bude toto dokonce zaměstnavatelova povinnost). Samozřejmostí potom je, že by zaměstnanci měli být s těmito pravidly a důvody také seznámeni. Takovýto postup jistě zamezí značnému množství sporů a nedorozumění.

Pokud jde o jednotlivé cíle sledované zaměstnavatelem, asi nejméně problematickým bodem bude bezpečnost. Není pochyb o tom, že zaměstnavatel je povinen zajistit bezpečné pracoviště,[239] ani o tom, že zaměstnanci jsou povinni příslušné pokyny a pravidla dodržovat.[240] Jak bylo uvedeno výše, zaměstnavatel bude v této situaci vždy povinen zaměstnancům toto transparentně a srozumitelně oznámit. Zároveň lze doporučit, aby daná omezení byla řádně zdůvodněna.

Pokud jde o vzhled pracoviště, tato otázka není zákonem nijak řešena. Nepochybně však ve většině případů bude mít zaměstnavatel právo o vzhledu pracoviště rozhodovat,[241] jelikož vzhled často souvisí též s bezpečností (např. je důležité, aby se ve výrobních halách nepovalovaly cizí předměty a vše mělo svůj řád) nebo s obchodním tajemstvím či závazky zaměstnavatele, jako je například mlčenlivost (uklizená kancelář, kde se nepovalují různé dokumenty) či jiné smluvní závazky (například závazky z franšízové smlouvy upravující vzhled prodejny či restaurace). V neposlední řadě může o vzhledu pracoviště rozhodovat také sám zaměstnavatel ze své vlastní vůle, zejména ve snaze vybudovat lepší image společnosti na pracovištích, kde zaměstnanci přichází do kontaktu se zákazníky či s klienty (například pobočky bank, energetických společností, telefonních operátorů, jakékoliv restaurace a prodejny apod.). Větší zásah do ochrany zaměstnanců v tomto ohledu není možné spatřovat. Zaměstnanci totiž takový postup očekávají (jsou s ním srozuměni ještě před nástupem na dané pracoviště) a nijak nevybočuje z běžného fungování společnosti. I v těchto případech jsou odpovídající požadavky na vzhled pracoviště obvykle upraveny ve vnitřních předpisech, ačkoliv s výjimkou požadavků bezpečnosti nejde o povinnost vyplývající z právních předpisů.

---

[239] Lze odkázat například na povinnosti týkající se BOZP (§ 101 a § 102 ZPr), povinnosti týkající se péče o zaměstnance (§ 224 odst. 1 ZPr), či samotné ustanovení dávající zaměstnavatelům možnost kontrolovat vnášené a odnášené předměty (§ 248 odst. 1 ZPr).
[240] Srov. ustanovení § 106 odst. 3 a 4 ZPr.
[241] Shodně Landwehrmann, T. *Kontrola vnášených a vynášených věcí na pracovišti*. Praktická personalistika. 2016, č. 7-8., s. 23.

Asi nejproblematičtější je, pokud zaměstnavatel zakazuje zaměstnancům vnášet na pracoviště předměty z důvodu ochrany svého majetku. Extrémním příkladem z praxe je třeba postup, kdy zaměstnavatel všem zaměstnancům přikazuje, aby odložili veškeré své osobní předměty do vyhrazených schránek a převlékli se do přiděleného pracovního úboru. K tomu dochází například ve skladových halách či jiných pracovištích, kdy je snadné cokoliv odcizit, a naopak velmi obtížné dohledat pachatele. Aby byl tento postup legitimní, je nutné dodržet několik zásad. Předně musí mít zaměstnavatel opravdový zájem na takovém opatření (například jsou u něho krádeže na denním pořádku). Dále nemůže existovat žádný jiný prostředek, kterým by bylo daného cíle dosaženo. V této souvislosti se nabízí možnost zavedení kamerového systému. Ta však bude vždy představovat ještě větší zásah do ochrany osobnosti zaměstnanců, a proto lze považovat systém převléknutí za vhodnější alternativu. Zaměstnanci by dále měli mít možnost vzít si určité nezbytné předměty s sebou (například mobilní telefon, léky, občerstvení), případně jim je zaměstnavatel musí zajistit (především již zmíněné občerstvení). Samozřejmostí by také v těchto situacích mělo být zajištění bezpečného úložiště pro ostatní osobní věci zaměstnanců a odpovídající převlékárny.

Nepochybně i v těchto případech bude muset daná pravidla upravovat vnitřní předpis zaměstnavatele, se kterým je zaměstnavatel povinen zaměstnance seznámit. Při splnění výše naznačených podmínek je možné dojít k závěru, že ani v těchto situacích nebude docházet k zásahům do ochrany osobnosti zaměstnanců. Pokud by však tyto podmínky splněny nebyly a zaměstnavatelovy úmysly by byly například šikanózní, nepochybně by se o nepřiměřený zásah do ochrany osobnosti zaměstnanců jednalo.

5.2 Obecné poznámky k ustanovení § 316 ZPr

Ustanovení § 316 ZPr, které je dále detailně analyzováno, je alfou a omegou ochrany soukromí zaměstnance v pracovněprávních vztazích. V odborné literatuře nepanují pochyby o tom, že jde o ustanovení relativně kogentní, tj. ustanovení od něhož se lze odchýlit pouze ve prospěch zaměstnance (s odkazem na ustanovení § 4a ZPr).[242] Bohužel u toho shoda obvykle končí, což lze s ohledem na důležitost tohoto ustanovení považovat za značný nedostatek, který by měl být do budoucna zákonodárcem jasně vyřešen. Jak bude vyplývat z další analýzy, autor této práce se zejména neshoduje s některými závěry podávanými

[242] Např. Štefko in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1242, Nonemann, F. *Soukromí na pracovišti*. Právní rozhledy. 2015, 23 (7), 229, nebo Morávek, J. *Sledování zaměstnanců v kontextu novely zákoníku práce*. Právní rozhledy. 2012, 20 (5), s. 175.

v komentářové literatuře[243] ani se závěry podanými v judikatuře Nejvyššího soudu.[244] Naopak za velmi kvalitní výklad autor této práce považuje časopisecký výklad podaný ze strany Morávka,[245] ač i vůči tomuto výkladu má autor této práce určité výhrady.

Je nepochybné, že ustanovení § 316 ZPr má též svébytný význam z hlediska zpracování osobních údajů zaměstnanců, neboť při kontrolách a sledování zaměstnanců bude vždy nevyhnutelně docházet také ke zpracování jejich osobních údajů. Morávek dokonce ustanovení § 316 ZPr považuje za právní předpis, resp. ustanovení, kterým členské státy mohou upravit podrobnější pravidla týkající se zpracování osobních údajů zaměstnanců ve smyslu čl. 88 nařízení GDPR.[246] Autor této práce se s tímto v zásadě neztotožňuje a domnívá se, že možnost danou čl. nařízení 88 GDPR by naplňovala jedině o poznání komplexnější úprava. K tomuto závěru se přiklonil též zákonodárce v důvodové zprávě k zákonu o zpracování osobních údajů, kde je jasně uvedeno, že tato možnost daná čl. 88 nařízení GDPR nebyla využita.[247] Ustanovení § 316 ZPr je spíše vhodné považovat za jakési minimum ochrany soukromí zaměstnanců (které by nadto bylo možné z větší části odvozovat z obecných principů či jiných pravidel).

V následujících podkapitolách je podán výklad o jednotlivých kontrolních oprávněních dle § 316 ZPr. Stranou je ponecháno ustanovení § 316 odst. 4, jehož zařazení v tomto ustanovení je přinejmenším nesystematické a které bylo analyzováno již výše v předcházející kapitole. Následuje též samostatná podkapitola věnující se postavení zaměstnavatele a analýze jeho důvodů pro provádění kontrol či sledování zaměstnanců. Závěry tam podané se přitom mohou vztáhnout rovnocenně též k předchozí podkapitole 5.1.

5.3 Kontrola svěřených prostředků

Je obvyklé, že zaměstnanci potřebují pro výkon práce určité prostředky, nástroje, zařízení, oděvy či jiné předměty. Může se jednat o vybavení kanceláře, dílny či jiného pracoviště, pracovní uniformu, nářadí, vozidlo, stroje, technologické nástroje, elektroniku, jako jsou počítače a jiná výpočetní technika, mobily a jiná telekomunikační zařízení, tablety

[243] Např. Štefko in Bělina, M. *Zákoník práce: komentář.* 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1239 a násl.
[244] Zejména v rámci rozhodnutí Nejvyššího soudu ČR ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011.
[245] Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 573 a násl. Případně obdobný výklad podaný v rámci knižní publikace Pichrt, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. Praha: Wolters Kluwer, 2017, (s. 943 a násl.).
[246] Tamtéž.
[247] Poslanecká sněmovna ČR, vláda ČR: Důvodová zpráva k zákonu č. 110/2019 Sb., zákon o zpracování osobních údajů.

a podobně. Může jít také o ochranné pracovní prostředky, které je zaměstnavatel dokonce povinen pro zaměstnance zajistit.[248] Protože by však dané prostředky zaměstnanci (obvykle) jinak nepotřebovali, musí jim je zajistit zaměstnavatel (přitom ale není rozhodné, zda budou takové prostředky v jeho vlastnictví nebo budou patřit třetí osobě, která je zaměstnavateli pouze poskytne dočasně k užívání).[249]

Jelikož se tedy nebude jednat o předměty, které by patřily zaměstnancům, je zaměstnavateli dáno oprávnění rozhodovat o tom, jak bude s těmito předměty nakládáno. Zejména je oprávněn určit, že tyto předměty mohou být využívány výhradně k výkonu práce. Dokonce i když zaměstnavatel žádné rozhodnutí neučiní, bude zaměstnancům jakékoliv jiné užívání pracovních prostředků zapovězeno. To totiž předpokládá zákon, když věta první ustanovení § 316 odst. 1 uvádí: *„Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení.“* Podle druhé věty téhož ustanovení přitom platí, že *„Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.“*.[250]

Pro úplnost výkladu je nutné doplnit, že je zákonnou povinností zaměstnanců ony svěřené prostředky k výkonu svěřených prací využívat a řádně s nimi hospodařit.[251] Zaměstnanci jsou vedle toho též povinni zaměstnavatelův majetek (tj. nejen svěřené prostředky) střežit a ochraňovat před poškozením, ztrátou, zničením či zneužitím.[252] Pokud by takto svěřené prostředky nevyužívali, pravděpodobně by to mohlo vést k rozvázání pracovního poměru. To však není předmětem zkoumání této práce. Naopak předmětem zkoumání je již výše zmíněná druhá věta ustanovení § 316 odst. 1 ZPr opravňující zaměstnavatele kontrolovat užívání svěřených prostředků.

---

[248] Srov. ustanovení § 104 ZPr.

[249] Bez ohledu na to není ani vyloučeno, aby zaměstnanci využívali k výkonu práce prostředky, které jsou v jejich soukromém vlastnictví, dohodnou-li se na tom se zaměstnavatelem. V takovém případě se však dle názoru autora této práce nebude aplikovat dále popisované ustanovení § 316 odst. 1 ZPr, jelikož dané ustanovení míří na ochranu zaměstnavatelova majetku (tím nicméně nebudou dotčena jiná ustanovení ZPr umožňující kontrolovat zaměstnancův řádný výkon práce). V odborné literatuře se však lze setkat i s odlišným názorem. Například Morávek dovozuje přiměřenou použitelnost ustanovení § 316 odst. 1 ZPr i na tyto případy, kdy zaměstnanec k výkonu práce využívá své vlastní prostředky (srov. Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 575).

[250] Srov. ustanovení § 316 odst. 1 ZPr.

[251] Srov. ustanovení § 301 písm. b) a d) ZPr.

[252] Srov. ustanovení § 301 písm. d) ZPr.

Pokud jde o otázku, diskutovanou v odborné literatuře,[253] zda musí zaměstnavatel za určitých okolností tolerovat využití svěřených prostředků pro osobní potřebu, autor této práce se ztotožňuje se závěrem, že toto povinnost zaměstnavatele rozhodně není. Jde o jím vlastněné či pro zaměstnance jinak obstarané prostředky, které zaměstnanci smějí využívat jen v souladu a za podmínek definovaných zaměstnavatelem. Pro jiné využití ze strany zaměstnanců nelze nalézt oprávněné argumenty a nic na tom nezmění skutečnost, že zaměstnanci mají legitimní očekávání soukromí na pracovišti (nemají totiž legitimní očekávání využití cizích nástrojů pro své osobní potřeby). Jiná je však situace, pokud by zaměstnavatel svolení udělil alespoň mlčky (srov. další výklad). Dříve uvedené samozřejmě neplatí rovněž pro využití v mimořádných situacích, ve stavu nouze či v naléhavém veřejném zájmu.[254]

5.3.1 Zákaz využívání

Z výše uvedeného je patrné, že zákon dává zaměstnavateli několik možností, jak k užívání výrobních a pracovních prostředků přistoupit. První situací, která bude obvykle častější, je situace, kdy mají zaměstnanci využívání těchto prostředků pro svou osobní potřebu zakázáno. Je zřejmé, že tato situace může nastat v návaznosti na dva různé přístupy zaměstnavatele. Jedním z nich je, že zaměstnavatel využívání pracovních a výrobních prostředků pro osobní potřebu zcela opomíjí. Pak se uplatní zákonem presumovaný zákaz a obecně by nemělo být pochyb[255] o tom, že zaměstnanci je pro osobní potřebu využívat nemohou.

Ještě snad méně pochyb bude v případě, že zaměstnavatel zaměstnancům užívání výrobních a pracovních prostředků pro osobní potřebu explicitně zakáže. To zaměstnavatel může udělat několika různými způsoby. Předně to může zaměstnancům zakázat v rámci pracovní smlouvy nebo v rámci interních předpisů, se kterými budou zaměstnanci povinni se seznámit. Není nicméně vyloučen ani jiný způsob, včetně samostatného oznámení doručeného zaměstnanci. S ohledem na presumovaný zákaz by bylo možné se domnívat, že explicitní zákaz je nadbytečný. S tím však lze v dnešní době do značné míry polemizovat a může nastat několik při nejmenším sporných situací, když se k této otázce zaměstnavatel

[253] Srov. Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 576.
[254] Srov. ustanovení § 1037 ObčZ.
[255] Formulace, že „*obecně by nemělo být pochyb*“ je zvolena záměrně, neboť autor této práce se domnívá, že v daném případě jisté pochybnosti vzniknout mohou (srov. další výklad).

nijak nepostaví. Před zmíněnou polemikou lze ještě pro úplnost vyslovit názor, že explicitní vyslovení zákazu je též v souladu s principy transparentnosti, obecné informační povinnosti a odpovědného přístupu zaměstnavatele vůči svým zaměstnancům.[256]

Pokud jde o sporné případy, kdy se zaměstnavatel k této otázce nijak nepostaví, může nastat zejména případ, že zaměstnavatel mlčky toleruje využívání daných prostředků pro osobní potřebu. Nabízí se pak otázka, zda lze takovou tichou akceptaci považovat za souhlas. Z hlediska právní teorie by bylo pravděpodobně možné označit takové jednání zaměstnavatele za konkludentní souhlas a dovozovat, že věta první § 316 odst. 1 ZPr se neuplatní, jelikož byl souhlas udělen. Takovýto závěr však nabízí řadu dalších otázek, na které rozhodně není jednoduché odpovědět. Jak se bude moci zaměstnanec bránit, pokud zaměstnavatel otočí a rázem přestane zaměstnancovo užívání svěřených prostředků pro osobní potřebu tolerovat?[257] Z hlediska právní teorie by takové chování zaměstnavatele bylo možné nepochybně považovat za odvolání souhlasu. Zásadní problém však může být ryze praktický, a to způsob, jakým by se zaměstnanec mohl proti takovémuto jednání zaměstnavatele bránit a jak by mohl dokazovat, že souhlas mu byl mlčky udělen.

Jinou situací, která může vyvolávat rovněž pochybnosti, je stav, kdy zaměstnavatel osobní užívání svěřených prostředků ani mlčky netoleruje, zejména z toho důvodu, že o něm neví, nicméně z hlediska zaměstnance by mohlo být legitimní očekávat, že daný pracovní prostředek je mu svěřen též pro osobní potřebu. Mohlo by jít například o situaci, kdy má zaměstnanec svěřeny zvláštní pracovní nástroje, které po pracovní době využije pro osobní potřebu.

Právní doktrína na výše uvedené situace obvykle žádný pohled nenabízí.[258] Podle názoru autora této práce bude odpověď na výše uvedené otázky spíše v neprospěch zaměstnance s ohledem na explicitní zákaz uvedený v dotčeném zákonném ustanovení. Zejména pokud jde o druhou z výše popsaných situací (kdy zaměstnavatel o ničem neví), pravděpodobně nebude možné, aby nastal případ, kdy by měl zaměstnanec v takové situaci

---

[256] Ač tuto povinnost asi není možné dovodit z žádného ustanovení ZPr upravujícího informační povinnost zaměstnavatele (zejména ustanovení § 37 ZPr), jelikož takový výklad by byl příliš extenzivní, nepochybně ani nelze dovozovat, že zaměstnavatel by opominutím této otázky (nevyslovením explicitního zákazu) zaměstnancům automaticky dovoloval výrobní a pracovní prostředky pro osobní potřeby užívat, neboť i takový výklad by byl přespříliš extenzivní a přímo by odporoval znění zákona.

[257] Dalšími otázkami by pak bylo, do jaké míry je zaměstnavatel oprávněn takové užívání kontrolovat a zda má zaměstnavatel možnost mlčky též určovat limity tohoto užívání (k tomu srov. další výklad).

[258] Výjimkou je například Morávek, který dovozuje oprávnění zaměstnavatele kontrolovat nakládání se svěřenými prostředky i mimo pracovní dobu. Zároveň však dodávají, že v takovém případě je nutné reflektovat, že mimo pracovní dobu má zaměstnanec nárok čekat vyšší míru soukromí (srov. Morávek in Pichrt, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. Praha: Wolters Kluwer, 2017, s. 948.).

rovněž legitimně očekávat, že daný nástroj může využít – v těchto případech si totiž vždy bude plně uvědomovat, že daná věc není jeho a používá ji bez svolení a vědomí zaměstnavatele. Složitější je však situace v případě tacitního tolerování. V takové situaci, lze mít minimálně z hlediska morálky a etiky pochybnosti o závěru, který by byl v neprospěch zaměstnance. Nabízí se proto otázka, zda by nebylo vhodné *de lege ferenda* uvažovat o zavedení zákonné presumpce chránící zaměstnance. Taková presumpce by přitom mohla v takovýchto sporných situacích (udělení souhlasu mlčky a legitimní očekávání zaměstnance) přenášet důkazní břemeno na zaměstnavatele o tom, že daný zákaz mlčky neudělil, resp. že zaměstnanec rozhodně nemohl mít příslušné legitimní očekávání o tom, že dané prostředky může užívat. Takové ustanovení by lépe chránilo zaměstnance, nepřímo by nutilo zaměstnavatele se k této otázce vyjádřit, ale zároveň by jim toto ani nadále nebylo uloženo (s tím, že sporné situace by šly k jejich tíži).

Závěrem lze ještě uvést, že úplné otočení zákonné presumpce, která je vyjádřena v první větě ustanovení § 316 odst. 1 ZPr tak, že by zaměstnancům bylo obecně dovoleno využívat svěřené prostředky pro osobní potřebu, rozhodně není vhodné, jelikož by příliš zatěžovalo drobné zaměstnavatele, a především by pravděpodobně bylo shledáno za rozporné s ústavním právem zaměstnavatele na ochranu jeho majetku a vlastnictví.

5.3.2 Dovolené využívání

Druhým a na první pohled méně komplikovaným postojem zaměstnavatele k využívání výrobních a pracovních prostředků je situace, kdy zaměstnavatel takové využívání pro osobní potřebu dovolí. Zaměstnavatel má jistě několik různých možností, jak toto zaměstnancům dovolit. Může se jednat o generální či obecné svolení vůči určitým výrobním a pracovním prostředkům obsažené ve vnitřním předpisu zaměstnavatele, může jít o konkrétní dovolení vztahující se ke konkrétnímu svěřenému prostředku obsažené v pracovní smlouvě nebo může jít o ad hoc udělený souhlas.

Dokonce není stanovena ani forma, jakou by takové dovolení zaměstnancům mělo být uděleno, a do úvahy připadá například ústní udělení souhlasu. Nepochybně by však mělo být preferovanou formou dovolení písemné, u kterého bude nižší pravděpodobnost vzniku sporu. Ostatně udělení ústního souhlasu je svojí důkazní silou v podstatě naroveň udělení souhlasu mlčky, které bylo popisováno výše a u kterého vzniká řada problémů, zejména možnost doložení souhlasu ze strany zaměstnance a jeho ochrana před náhlou změnou názoru zaměstnavatele.

Pokud jde o otázku obsahu souhlasu, je nepochybné, že souhlas nemusí být udělen jen v tom smyslu, zda užívání daných prostředků je dovoleno či zakázáno, ale zaměstnavateli je dána možnost definovat podmínky takového užívání pracovních a výrobních prostředků zaměstnanci. Tento názor zastává též judikatura, srov. rozhodnutí Nejvyššího soudu ČR ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011, v rámci kterého bylo dovozeno, *že „protože zákonem stanovený zákaz používat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele je absolutní, může zaměstnavatel souhlas k jejich použití stanovit v libovolném rozsahu (od úplného souhlasu bez jakéhokoli omezení, přes souhlas jen v určitém rozsahu časovém nebo věcném, až třeba po souhlas jen k jednorázovému použití). Stanovení rozsahu souhlasu k použití výrobních a pracovních prostředků zaměstnavatele pro osobní potřebu zaměstnance (zaměstnanců) je zcela na vůli zaměstnavatele.“*.

Další důležitou otázkou je, do jaké míry bude kontrolní oprávnění zaměstnavatele ovlivněno v závislosti na tom, zda zaměstnavatel dovolí svým zaměstnancům výrobní a pracovní prostředky užívat též pro osobní potřebu. V ustanovení § 316 odst. 1 věta druhá se jasně uvádí, že dodržování zákazu podle věty první je zaměstnavatel oprávněn kontrolovat. Ale uplatní se takovéto oprávnění zaměstnavatele provádět kontrolu i na situace, které jdou nad rámec „věty první“ a kdy zaměstnanci dotčené prostředky pro osobní potřebu užívat mohou? Autor této práce se kloní k možnosti, že ano. Předně platí výše uvedený závěr týkající se toho, že zaměstnavatel je oprávněn definovat podmínky užívání pro osobní potřebu, a nepochybně tedy má i možnost určit jako jednu z podmínek své oprávnění ke kontrole. Toto však není nezbytné a jeho oprávnění ke kontrole bude podle názoru autora této práce obsaženo v již každém obecném dovolení. Lze totiž vyjít z argumentace od většího k menšímu, a pokud má zaměstnavatel oprávnění kontrolovat obecný zákaz, musí mít možnost kontrolovat i jím zmírněný zákaz. I nadále totiž platí, že zaměstnavatel je tím, kdo má vlastnické právo k dané věci a rozhoduje o tom, jak s ní může být nakládáno.[259]

5.3.3 Přiměřený způsob kontroly

Asi nejsložitější při rozboru možnosti užívání svěřených výrobních a pracovních prostředků je otázka, co znamená přiměřený způsob kontroly, který je zaměstnavatel

[259] Pokud jde o otázku, co by měl zaměstnavatel kontrolovat a zda je vůbec co kontrolovat, když zaměstnanec může svěřené prostředky využívat pro osobní potřebu, platí, že i v takových situacích má kontrola samozřejmě význam. Například totiž neplatí, že pokud jsou prostředky svěřeny zaměstnanci k užití pro jeho osobní potřebu, může ten dále svobodně rozhodovat o využívání svěřeného prostředku ze strany dalších osob.

oprávněn provádět ve smyslu ustanovení věty druhé § 316 odst. 1 ZPr.[260] Jistě není pochyb o tom, že zaměstnavatel není povinen toto své právo využívat. Pokud by ho neuplatňoval, mohlo by nicméně být za určitých okolností sporné, zda je užití pracovních prostředků pro osobní užití skutečně zakázáno (nezakázal-li zaměstnavatel explicitně užití pro osobní potřebu). Blíže k této otázce viz výše v bodě 5.3.1.

Zákon nijak nedefinuje ani blíže nevymezuje, co se rozumí přiměřeným způsobem kontroly. Je však nepochybné, že v tomto ohledu bude muset postupovat velmi citlivě, protože jde v podstatě o balancování mezi dvěma právy, a to ochranou majetku a ochranou soukromí. De facto tak bude muset být prováděn test proporcionality, v rámci kterého bude nutné posoudit celou řadu aspektů. Morávek v této souvislosti správně poznamenává, že *„zmocnění zaměstnavatele ke kontrole je v návaznosti na čl. 4 Listiny třeba vyložit v souladu s principem nezbytnosti tak, že zásah do chráněných zájmů zaměstnance je možný při splnění zákonem předepsaných podmínek […], musí však být proveden jen v nezbytně nutném rozsahu“*.[261] S tím se lze jednoznačně ztotožnit.

Obecně lze v souvislosti s principem nezbytnosti uvést, že zaměstnavatel bude muset mít nepochybně legitimní cíl pro provedení kontroly. Ačkoliv s jeho určením obvykle nebude problém (když půjde jednoduše o ochranu majetku zaměstnavatele), složitějším úkolem bude jeho poměření s právem zaměstnance na ochranu soukromí. Zaměstnavatel by za všech okolností měl být schopen prokázat, že zvolené metody kontroly jsou schopné vést k požadovanému cíli (nejsou tedy jen spekulativní) a že jsou využívány jen v nezbytném rozsahu. Rovněž by měl být dodržen princip subsidiarity a zaměstnavatel by měl volit jen takové prostředky, které budou při splnění vytyčeného cíle (ochrany jeho majetku) v co nejmenším rozsahu zasahovat do ochrany osobnosti zaměstnance.

Otázkou přiměřeného rozsahu kontroly se zabýval též Nejvyšší soud ČR, a to ve svém výše zmíněném rozhodnutí ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011, v rámci kterého se zabýval též otázkou ochrany osobnosti zaměstnance. V daném rozhodnutí Nejvyšší soud zejména uvedl, že *„protože zákon blíže nestanoví, co je oním přiměřeným způsobem kontroly, jedná se o právní normu s relativně neurčitou (abstraktní) hypotézou, tj. o právní normu, jejíž hypotéza není stanovena přímo právním předpisem a která tak přenechává soudu, aby podle svého uvážení v každém jednotlivém případě vymezil sám*

[260] Podle tohoto ustanovení platí, že: „*Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.*“

[261] Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 576.

hypotézu právní normy ze širokého, předem neomezeného okruhu okolností. Přitom soud patrně přihlédne zejména k tomu, zda šlo o kontrolu průběžnou či následnou, k její délce, rozsahu, k tomu, zda vůbec a do jaké míry omezovala zaměstnance v jeho činnosti, zda vůbec a do jaké míry zasahovala také do práva na soukromí zaměstnance apod.“. Na druhou stranu soud rovněž konstatoval, že ochrana zaměstnanců nemůže být absolutní, když prohlásil, že *„zároveň je třeba mít na zřeteli, že, má-li zaměstnanec zakázáno užívat majetek zaměstnavatele pro svou osobní potřebu a zaměstnavatel má právo kontrolovat dodržování tohoto zákazu, musí mít zaměstnavatel také možnost nějakým způsobem tuto kontrolu realizovat a získat případně důkaz o nedodržování uvedeného zákazu“*. Tím soud naopak zdůraznil také důležitost ochrany majetku zaměstnavatele a její legitimnost vůči ochraně osobnosti zaměstnance.

Kromě výše uvedeného se Nejvyšší soud vyjádřil také k otázce toho, co vše může zaměstnavatel kontrolovat a ve stejném rozhodnutí dovodil, že *„předmětem kontroly samozřejmě může být toliko zjištění, zda zaměstnanec porušil zákonem stanovený absolutní zákaz, ale s přihlédnutím k tomu, zda […] zaměstnavatel neučinil souhlas používat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky a jeho telekomunikační zařízení a v jakém rozsahu; půjde tedy jen o kontrolu nedodržení těch povinností, jež nebyly zaměstnavatelem vyloučeny nebo zmírněny“*. Je proto zřejmé, že pokud by zaměstnavatel zaměstnancům dovolil svěřené výrobní a pracovní prostředky užívat kdykoliv a jakkoliv pro soukromé účely, měl by jen velmi omezený prostor pro kontrolu.[262]

Popisované rozhodnutí Nejvyššího soudu lze, bohužel, označit za judikatorní vlaštovku v této oblasti.[263] A jelikož se obdobné spory dostanou až k Nejvyššímu soudu jen málokdy, lze ocenit skutečnost, že soud poskytl alespoň určitá vodítka k výkladu tohoto ustanovení. Z hlediska každodenní praxe má nepochybně také význam zaobírat se názorem orgánu, který je pověřen kontrolou dodržování tohoto ustanovení. Tímto orgánem je

[262] Dalo by se uvažovat o možnosti zaměstnavatele kontrolovat, zda například nedochází k neúměrnému opotřebování či poškozování svěřených prostředků. Taková kontrola by však byla mimo rámec § 316 odst. 1 ZPr, a nemělo by při ní tudíž (s ohledem na oprávnění svěřená zaměstnanci) nikdy docházet k zásahům do ochrany osobnosti zaměstnanců.

[263] Přestože Nejvyšší soud ČR řešil výklad těchto ustanovení i v navazujících rozhodnutích, vždy se již pouze omezil na odkaz na dříve citované rozhodnutí a zatím se nepustil do dalších úvah o jeho obsahu (srov. např. rozhodnutí Nejvyššího soudu ČR ze dne 7. srpna 2014, sp. zn. 21 Cdo 747/2013).

inspekce práce.[264] Podle veřejně dostupných informací se, ke škodě věci, tento orgán zatím nepustil do bližšího rozboru tohoto ustanovení, pouze na svém webu v rámci sekce otázek a odpovědí k monitorování prostřednictvím kamerového systému a k ustanovení § 316 odst. 1 ZPr uvádí, že *„přiměřenost takovéto kontroly je vždy potřeba hodnotit ve vztahu ke konkrétnímu pracovišti a konkrétnímu zaměstnanci. Zpravidla ale nepůjde o přiměřenou kontrolu v případě trvalého sledování zaměstnance a jeho nakládání se svěřenými pracovními prostředky.“*.[265]

Snad je to dáno relativně krátkou dobou, kdy je tento orgán pověřen kontrolou dodržování tohoto ustanovení, nicméně lze vyjádřit určitou lítost nad tím, že ze strany tohoto orgánu nejsou zaměstnavatelům poskytnuta bližší vodítka k dodržování předmětného ustanovení, a zaměstnavatelům proto nezbude než vycházet z výše citovaného rozhodnutí Nejvyššího soudu. Tímto rozhodně nemá být nikterak zpochybňována právní relevantnost, vážnost a přesvědčivost závěrů poskytnutých Nejvyšším soudem, bylo by však minimálně dobrou praxí a službou ze strany veřejného orgánu, pokud by tento orgán alespoň určitá vodítka poskytl. Obzvláště v situaci, kdy výklad ustanovení § 316 ZPr rozhodně není jednoduchý.

Závěrem této podkapitoly ještě poznámka k praktickému významu ustanovení § 316 odst. 1 ZPr. Autor této práce se rozhodně nedomnívá, že by předmětné ustanovení bylo nadbytečné. K částečně odlišným závěrům dochází nicméně Morávek, který uvádí, že shodné závěry plynou *„z povahy věci z podstaty vlastnického práva a práva na ochranu majetku“*.[266] Přitom dodává, že má na mysli ochranu majetku zaměstnavatele v širším smyslu a nemusí jít vždy o majetek zaměstnavatele, ale mohou být zahrnuty též náklady na dispozice s těmito věcmi apod.[267] Podle názoru autora této práce bylo nicméně jasně ukázáno, že právě v oblasti pracovního práva je nutné blíže vymezit ochranu práv zaměstnance s ohledem na silnější postavení zaměstnavatele. Byť je toto v předmětném ustanovení vyjádřeno toliko slovním spojením, že zaměstnavatel je oprávněn *„přiměřeným způsobem kontrolovat“* dodržování zákazu, s pomocí výkladu lze dovozovat snahu

---

[264] Byla tristní skutečnost, že před datem 29. července 2017 nebyl jasně určen orgán, který by na dodržování těchto povinností dohlížel. Toto bylo prosazeno až na základě novely zákona o inspekci práce, zákonem č. 206/2017 Sb.

[265] Státní úřad inspekce práce. *Monitorování zaměstnanců na pracovišti kamerovým systémem. Otázky a odpovědi* [online]. Přidáno dne 7. dubna 2014. [cit. 2019-02-27]. Dostupné z: http://www.suip.cz/otazky-a-odpovedi/pracovnepravni-vztahy/ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance/monitorovani-zamestnancu-na-pracovisti-kamerovym-systemem-pridano-7-4-2014/

[266] Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 575.

[267] Tamtéž.

zákonodárce postavení zaměstnance vůči zaměstnavateli alespoň do určité míry posílit. Naopak by podle názoru autora této práce mělo být toto ustanovení dále rozšířeno, a to ve smyslu výše uvedených doporučení.

5.4 Kontrola, existuje-li závažný důvod

Dalším kontrolním oprávněním, které má zaměstnavatel vůči svým zaměstnancům a které je relevantní z hlediska ochrany osobnosti zaměstnanců, je kontrolní oprávnění podle § 316 odst. 2 ZPr. Podle tohoto ustanovení platí, že *„zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci“*. Dále je postupně zkoumán vztah tohoto ustanovení s odstavcem § 316 odst. 1 ZPr, výkladové nejasnosti týkající se tohoto ustanovení, ale také navazující ustanovení § 316 odst. 3 ZPr a otázky spojené s aplikací tohoto ustanovení v praxi.

5.4.1 Vzájemný vztah kontrolních oprávnění

Před důkladnou analýzou a výkladem o jednotlivých pojmech naposledy citovaného ustanovení, jejich obsahu a slovním a jiném významu je ještě nutné se zabývat jeho koncepčním zařazením v rámci § 316 ZPr a obecným výkladem v souvislosti s jinými kontrolními oprávněními zaměstnavatele. Platí přitom, že vyjasnění této otázky je klíčové pro správné chápání a aplikaci tohoto ustanovení. Ač by se mohlo zdát, že jde o snadnou otázku, rozhodně tomu tak není. S ohledem na systematické zařazení tohoto kontrolního oprávnění v ustanovení § 316 ZPr se totiž nabízí hned několik možných odpovědí.

První variantou je, že dané kontrolní oprávnění podle druhého odstavce § 316 ZPr navazuje na první odstavec a rozvíjí jej. Tomuto výkladu by mohlo nasvědčovat především systematické zařazení v rámci § 316 ZPr. Tento názor byl v podstatě vyjádřen v judikatuře Nejvyššího soudu ČR, a to v rámci výše citované rozhodnutí 21 Cdo 1771/2011. V něm Nejvyšší soud k § 316 odst. 2 ZPr uvedl, že *„uvedené ustanovení v první řadě dopadá toliko na případy zvláštní povahy činnosti zaměstnavatele (což v projednávané věci nebylo ani tvrzeno) a navíc se vztahuje jen na situace, kdy zaměstnanec buď se souhlasem zaměstnavatele používá pro svou osobní potřebu zaměstnavatelovy výrobní a pracovní prostředky (jak shora popsáno), nebo z nějakého důvodu používá u zaměstnavatele své*

vlastní výrobní a pracovní prostředky včetně výpočetní techniky či telekomunikačního zařízení (vlastní PC, notebook, mobilní telefon, psací stroj apod.) a na všechny předměty a projevy (soukromé povahy) zaměstnance“.

Druhou variantou je v podstatě úplné oddělení jednotlivých kontrolních oprávnění zaměstnavatele podle § 316 odst. 1 a 2 ZPr nehledě na jejich systematické zařazení. Tento názor nepochybně zastává Morávek, který k věci uvádí: *„Ustanovení § 316 odst. 2 ZPr by mělo být aplikováno jak v případech realizace účelu, jímž je ochrana majetku zaměstnavatele v užším smyslu slova, tj. ochrana prostředků ve smyslu § 316 odst. 1 ZPr (viz shora), tak i na ostatní případy kontroly plnění pracovních povinností zaměstnance.*[268] Morávek tedy výklad staví na právu zaměstnavatele na ochranu jeho majetku, který je možné chápat v užším smyslu (jen svěřené výrobní a pracovní prostředky) a ve smyslu širším (jakékoliv jiná kontrola zaměstnance a narušování). Morávek k tomu dodává, že *„výlučně podle § 316 odst. 1 se postupuje, je-li pravděpodobné […], že nemůže dojít k narušení soukromí zaměstnance, bez ohledu na zvolený prostředek kontroly. Dále se výlučně podle tohoto ustanovení postupuje, i kdyby docházelo k zásahu do soukromí zaměstnance, je-li zvolena jiná forma kontroly nežli ta, kterou vypočítává § 316 odst. 2 […]; příkladem může být nahlédnutí do knihy jízd služebního vozu či jiná nahodilá kontrola realizovaná v reálném čase, jde-li o ad hoc případy. V případech ostatních se použije § 316 odst. 1 ve spojení s § 316 odst. 2, 3 ZPr“.*[269]

Autor této práce se jednoznačně přiklání k druhé z variant, nicméně s určitou výhradou (viz dále). Kontrolní oprávnění dle § 316 odst. 1 a odst. 2 ZPr chápe jako dvě samostatné množiny, které se mohou, ale nemusí překrývat. Předně platí, že pro provádění kontroly dle ustanovení § 316 odst. 1 ZPr zaměstnavateli nemusí mít zaměstnavatel tzv. závažné důvody spočívající ve zvláštní povaze činnosti zaměstnavatele, jak požaduje druhý odstavec. Naopak kontrolní oprávnění dle druhého odstavce není omezeno jen na ochranu svěřených prostředků, ale může sledovat též jiné zájmy zaměstnavatele či obecné zájmy (jako je například bezpečnost).

Kromě uvedeného nicméně autor této práce dovozuje i třetí množinu kontrolních oprávnění zaměstnavatele, která vůbec není vyjádřena v § 316 ZPr. Podle autora této práce totiž může nastat rovněž situace, ve které zaměstnavatel bude zasahovat svou kontrolou do soukromí zaměstnance, nebude však vykonávat kontrolu svěřených výrobních a pracovních

---

[268] Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 577.
[269] Tamtéž.

prostředků (potažmo ochranu svého majetku) ve smyslu odst. 1, a ani nebude zvolena kontrolní metoda, na kterou míří ustanovení odstavce druhého.[270] Mohlo by se jednat například o zaměstnavatelem prováděnou kontrolu jiného jeho majetku, který nebyl svěřen zaměstnanci, ale při kontrole bude (například protože je to nevyhnutelné) zasaženo do ochrany soukromí zaměstnance.

Ať už je objektivní správnost výkladu ustanovení § 316 ZPr jakákoliv, je nepochybné, že výklad tohoto ustanovení není jednoduchý a de lege ferenda by bylo vhodné dané ustanovení novelizovat, aby se tyto výkladové nejasnosti odstranily. Za zmínku ještě stojí skutečnost, že druhou variantu výkladu podpořil též ÚOOÚ. Ten se ve svém rozhodnutí č. j. UOOU-00237/13-38, ze dne 3. 7. 2013, zabýval otázkou využívání sledování zaměstnanců pomocí GPS, které mělo být prováděno primárně za účelem optimalizace doručování (zaměstnavatelem byla Česká pošta). Ačkoliv se tedy v daném případě nejednalo o situaci, kdy by zaměstnavatel využíval sledovacího nástroje, aby kontroloval, jak využívají svěřené prostředky (cílem byla zmiňovaná optimalizace), ÚOOÚ dovodil nezbytnost aplikace § 316 odst. 2 ZPr s ohledem na zvolené sledovací mechanismy a zásah do soukromí zaměstnanců.[271]

5.4.2 Podmínky pro aplikaci kontrolního oprávnění

Ze zkoumaného ustanovení § 316 odst. 2 ZPr je zřejmé, že kontrolní oprávnění přiznané zaměstnavateli je velmi limitováno. Zaměstnavatel může takové kontroly provádět jen v situaci, kdy existuje *„závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele“*. Zákonodárce záměrně tento termíny nijak nedefinuje a dává tak prostor pro volné uvážení o jeho obsahu. To má své výhody (ustanovení není zbytečně rigidní a výklad těchto podmínek se může měnit s ohledem na různé faktory) i nevýhody (neexistuje právní jistota, kdy jsou tyto podmínky naplněny). Problém je navíc umocněn tím, že je v daném spojení použito více neurčitých termínů.[272] Samozřejmým důsledkem je, že se rozbíhají názory na to, co jsou ony závažné důvody, resp. co je zvláštní povaha zaměstnavatele.

---

[270] Zaměstnavatel tedy nebude podrobovat zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.

[271] Pro úplnost lze uvést, že tento výklad, tj. že správná je druhá z variant, lze podpořit též skutečností, že v rámci ustanovení § 316 ZPr je zařazen též zcela nesystematický odstavec čtvrtý, a tak lze snadno vést pochybnosti o tom, že by ustanovení § 316 ZPr mělo tvořit jednotný celek.

[272] Pravděpodobně méně sporným bude výklad toho, co je *„závažný důvod“*, naopak výklad toho, co je *„zvláštní povaha zaměstnavatele“* bude činit více problémů.

Například Štefko uvádí, že závažnými důvody může být ochrana života a zdraví zaměstnavatele, zaměstnanců či jiných osob nebo ochrana majetku. Dokonce též kontrola pracovní výkonnosti zaměstnance. Zároveň odmítá názor, že by právo na kontrolu měli pouze zaměstnavatelé vykonávající činnosti zvlášť nebezpečné (např. jaderné elektrárny).[273] Radičová poté k pojmu zvláštní činnost zaměstnavatele shrnuje, že by se obecně mělo jednat *„o činnosti se zvýšeným nárokem na chování zaměstnanců, kde je zavedení sledovacího mechanismu objektivně odůvodnitelné, např. s ohledem na ochranu práv a majetkových zájmů zaměstnavatele“*.[274] Morávek poněkud blíže vysvětluje, co by mělo být oním závažným důvodem, a dovozuje, že pro objektivní posouzení této otázky bude nutné provést test přiměřenosti, v rámci kterého budou poměřovány zájmy zaměstnavatele na ochranu majetku a zaměstnance na ochranu soukromí.[275] Naopak se zároveň zdráhá učinit jakoukoliv definici toho, co by mělo být onou zvláštní činností zaměstnavatele, když uvádí, že toto bude nutné ad hoc zkoumat, a dokonce se může *„jednat o činnost vrcholového manažera, který disponuje širokými rozhodovacími kompetencemi ve vztahu k majetku zaměstnavatele a dispozičními právy k bankovním účtům, stejně tak jako o činnost zaměstnance ve výrobě, který má přístup k jádru obchodního tajemství […]“*.[276]

Nonnemann k této otázce uvádí, že *„pro zahájení sledování určitého zaměstnance nebo skupiny zaměstnanců je nezbytné, aby v předmětu jejich práce byl objektivně seznatelný důvod pro takovýto zásah do soukromí, přičemž tento důvod v obecné rovině vychází ze zvláštního předmětu činnosti zaměstnavatele“*.[277] Zároveň také ale uvádí, že *„zaměstnavatel, resp. předmět jeho činnosti jako takový, musí být v určitém směru specifický“*.[278] Tím se tedy značně odlišuje od názoru Morávka (a částečně i Štefka), který obecně takovouto specifičnost pro předmět činnosti zaměstnavatele nedovozuje. Odlišuje se též od názoru vyjádřeného ÚOOÚ. Ten se k této otázce vyjádřil ve výše citovaném rozhodnutí č. j. UOOU-00237/13-38, ze dne 3. 7. 2013, ve kterém uvedl: *„Dle názoru správního orgánu totiž nelze […] zvláštní povahu činnosti zaměstnavatele automaticky ztotožňovat se zaměstnavateli, jejichž činnost je upravena speciálními právními předpisy.“* Posuzovaná

---

[273] Štefko in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1243.
[274] Radičová, Z. *Monitoring zaměstnanců prostřednictvím GPS technologie*. Právní rozhledy. 2014. 22 (21), s. 737.
[275] Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 578.
[276] Tamtéž. Za zmínku stojí též názor Morávka, který se domnívá, že by z hlediska racionální aplikace daného ustanovení nemělo docházet k oddělování obou neurčitých pojmů (tj. závažné důvody a zvláštní povaha zaměstnavatele) na dvě samostatné podmínky, které by musely být splněny kumulativně.
[277] Nonemann, F. *Soukromí na pracovišti*. Právní rozhledy. 2015, 23 (7), s. 232.
[278] Tamtéž.

činnost byla přitom vykonávána u České pošty a z této samotné skutečnosti správní orgán neodmítl zabývat se otázkou, zda není namístě ustanovení §316 odst. 2 ZPr aplikovat. Pokud jde o judikaturu vyšších soudů, která by se k této otázce detailně vyjadřovala, ta bohužel zatím stále není dostupná.[279]

Dalo by se jistě dohledat mnoho dalších názorů na to, jak mají být tyto pojmy vykládány. To však není záměrem. Záměrem bylo nalézt shodné, odlišné nebo převažující prvky podávaných výkladů a případně poskytnout vlastní pohled na věc. Shodným prvkem by podle názoru autora této práce měla být především skutečnost, že oba neurčité pojmy je nutné vykládat ve vzájemné souvislosti. Zvláštní povahu činnosti zaměstnavatele nelze omezovat specifičností činnosti zaměstnavatele (např. na nebezpečné činnosti),[280] ale může být přiznána zaměstnavatelům vykonávajícím široké spektrum činností. Při určování závažných důvodů bude nutné vždy ad hoc poměřovat zájem zaměstnance na ochraně jeho soukromí vs. oprávněné zájmy zaměstnavatele (které však mohou být různé). Pokud budou brány v potaz tyto aspekty, mělo by vždy být možné závažné důvody zaměstnavatele spočívající v jeho zvláštní činnosti určit. V praxi by se podle názoru autora této práce mělo jednat především o pracovní pozice, kde je zaměstnancům svěřena velká odpovědnost a je objektivně zdůvodnitelné, aby k určitému sledování docházelo, například pozice pokladníka v bance (kamerové sledování), pozice IT administrátora významných systémů (logování), pozice řidičů nákladních vozů převážejících zboží značné hodnoty (GPS sledování) apod.

K výše uvedenému je ještě nutné doplnit jednu, ne na první pohled patrnou věc. Povaha zvoleného sledovacího prostředku zaměstnavatelem totiž může ovlivnit skutečnost, zda bude sledování přípustné ve smyslu § 316 odst. 2 ZPr či nikoliv. Toto vyplývá z výše zmíněné nutnosti poměřovat zájmy zaměstnavatele se zájmy zaměstnance na ochraně jeho soukromí. Přirozeně totiž při více intenzivním zásahu do soukromí zaměstnance bude nutná existence ještě významnějšího zájmu zaměstnavatele. Uvedené lze ilustrovat na výše zmíněném příkladu sledování řidičů nákladních vozů. Zatímco sledování pomocí GPS bude mnohdy přípustné, totéž již nemusí platit, pokud by měla být do kabiny řidiče nainstalována kamera.

---

[279] Částečně se této otázce věnovalo výše uvedené rozhodnutí Nejvyššího soudu ČR ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011. To však podle názoru autora této práce dovozuje ve vztahu k § 316 odst. 2 ZPr chybné závěry, jak bylo uvedeno výše. Otázka ochrany soukromí a výklad ustanovení § 316 ZPr byly rovněž předmětem rozhodnutí Nejvyššího správního soudu ČR ze dne 23. srpna 2013, sp. zn. 5 As 158/2012, ale ani v tomto případě nedošlo k bližšímu rozboru a analýze vztahů jednotlivých ustanovení v rámci § 316 ZPr.

[280] S výjimkou výše uvedeného názoru Nonnemanna.

Bohužel to však nemusí být jen zmíněné neurčité pojmy, které mohou činit výkladové potíže v rámci § 316 odst. 2 ZPr. Jistota nemusí panovat například u pojmu, dalo by se říci triviálního, kterým je pracoviště. ZPr tento pojem definuje pouze v rámci § 34a ZPr, avšak pouze pro účely cestovních náhrad, a toto vymezení tudíž není pro § 316 odst. 2 ZPr použitelné. Odrazit by se dalo od výkladu Běliny, který k pojmu pracoviště (ač právě při výkladu o § 34a ZPr) uvádí, že *„pojem pravidelné pracoviště ZPr nedefinuje, ale rozumí se jím určitý prostor, kde zaměstnanec má zpravidla vykonávat přidělenou práci (např. dílna, kancelář, staveniště)“*.[281] Spojíme-li toto s ustanovením § 316 odst. 2 ZPr, kde se vedle pojmu pracoviště používá též pojem společné prostory zaměstnavatele, můžeme zároveň dovodit, že pracovištěm nebudou veškeré prostory zaměstnavatele, ale jen ty, které jsou určeny pro výkon práce.

Výklad tohoto pojmu by tak neměl způsobovat větší aplikační obtíže, zejména s ohledem na skutečnost, že v rámci ustanovení § 316 odst. 2 ZPr není chráněno jen pracoviště, ale i ony společné prostory zaměstnavatele. Zaměstnavatel proto nemá příliš prostoru pro zužující výklad, který by byl v neprospěch zaměstnance. Pro úplnost je však nutné dodat, že sledování zaměstnance na pracovišti by mělo být obecně méně přípustné než sledování zaměstnanců ve společných prostorách zaměstnavatele. Vyjdeme-li totiž z premisy, že zaměstnanci tráví většinu pracovní doby na pracovišti, bude obecně rovněž platit, že sledováním zaměstnanců na pracovišti bude ve větší míře zasahováno do jejich práva na ochranu soukromí a bude tedy takové sledování obecně méně přístupné než sledování ve společných prostorech zaměstnavatele, kde se zaměstnanci pouze během pracovní doby mihnou.

5.4.3 Obsah kontrolního oprávnění

Ustanovení § 316 odst. 2 ZPR podává výčet kontrolních mechanismů, které jsou zaměstnavateli zapovězeny, resp. dovoleny jen při splnění výše rozebraných podmínek. Jedná se o otevřené nebo skryté sledování, odposlech a záznam telefonických hovorů zaměstnance, kontrola elektronické pošty nebo kontrola listovních zásilek adresovaných zaměstnanci. Jde o relativně široký výčet. Pokud by měla být zkoumána otázka, zda explicitní jmenování elektronické pošty, telefonických hovorů a listovních zásilek ukazuje, že se jedná o taxativní výčet, odpověď by podle názoru autora této práce mělá znít, že nikoliv. Jednak jde o ustanovení, které má chránit zaměstnance a je nutné jej vykládat v jeho

[281] Bělina in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 220.

prospěch. Tedy, čím širší výčet v ustanovení bude uveden, resp. z něj bude dovozován, tím větší ochrana bude zaměstnanci náležet. Snad ještě významnější je však skutečnost, že daná ustanovení se aplikují na veškeré případy „sledování“. To je na tolik široký pojem, že by pod něj nepochybně bylo možné vztáhnout i ostatní zmiňované mechanismy kontroly, kterými jsou odposlechy a záznam hovorů či kontrola pošty a listovních zásilek. Nebude ani pochyb o tom, že může jít o online kontrolu (kamery, odposlech, sledování užívání PC), nebo zpětnou kontrolu prostřednictvím pořízených záznamů. Jednotlivým, zaměstnavateli nejčastěji využívaným prostředkům kontroly se věnuje podkapitola 8.1.

Důležitou otázkou může být nicméně určení toho, zda existují nějaké mechanismy kontroly, na které by se dané ustanovení vztahovat nemělo, tedy prostředky kontroly, které by nebylo možné podřadit pod pojem sledování, a také otázka, jakou ochranu soukromí zaměstnanců bude nutné v takových situacích aplikovat. Morávek k pojmu sledování uvádí, že se jím rozumí *„delší dobu trvající nebo opakované systematické kontrolování zaměstnance prostřednictvím daného systému/prostředku (opačně, pokud bude on-line kamera určena primárně k jinému účelu a zaměstnavatel jejím prostřednictvím ad hoc zkontroluje zaměstnance, tj. způsobem nelišícím se od běžné kontroly vedoucím zaměstnancem v místě pracoviště, komentované ustanovení na tyto případy dopadat nebude)“*.[282]

Autor této práce se ztotožňuje se skutečností, že by se mělo jednat o soustavné či opakované systematické kontrolování, a se závěrem, že ne všechny prostředky kontroly bude možné a nutné zařazovat pod zkoumané ustanovení. Na druhou stranu není podaný příklad užívání online kamery příliš přesvědčivý. Pokud je totiž účelem kamerového systému kontrola bezpečnosti, neměl by být podle názoru autora této práce využíván pro jiné účely, a i v takovém případě bude potřeba aplikovat § 316 odst. 2 ZPr. Výjimkou by byla situace, pokud by toto bylo zaměstnanci předem oznámeno a zaměstnanec by mohl takovou kontrolu (legitimně) očekávat. Spíše by tedy bylo vhodné uvést příklad, kdy zaměstnavatel využije náhodně určitý kontrolní prostředek. Nejjednodušším příkladem může být náhodná osobní kontrola zaměstnance a kontrola jeho pracoviště ze strany nadřízeného.

5.4.4 Informační povinnost zaměstnavatele

Podle ustanovení § 316 odst. 3 ZPr platí, že pokud zaměstnavatel bude chtít zavést předmětné kontrolní mechanismy, je povinen zaměstnance přímo informovat o rozsahu

[282] Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 577.

kontroly a o způsobech jejího provádění.[283] Nejasnou otázkou v této souvislosti může být, kdy by měl zaměstnavatel tuto povinnost plnit, neboť ustanovení § 316 odst. 3 ZPr toto neurčuje. Ustanovení § 316 odst. 2 ZPr uvádí, že zaměstnavatel je při splnění stanovených podmínek oprávněn zavést otevřené i skryté sledování.[284]

U otevřeného sledování nebude pochyb o tom, že zaměstnanec o takovém sledování musí být jasně předem informován. Méně jasné může být plnění informační povinnosti v případě skrytého sledování. Podle názoru autora této práce však i v takovém případě musí zaměstnavatel své zaměstnance o možnosti takového sledování předem informovat. Nemusí jít o detailní informování o využitých prostředcích, rozsahu atd. (pak už by se přirozeně nejednalo o skryté sledování), ale mělo by jít alespoň o obecné informování o možné kontrole, které by též obsahovalo zdůvodnění, aby si zaměstnanec alespoň v hrubých rysech uměl udělat představu o skrytých kontrolách zaměstnavatele.[285] Jen takový závěr totiž koresponduje s principem legitimního očekávání, jak jej definuje ve své judikatuře ESLP. Jen v případě, kdy bude zaměstnanec o možných kontrolách informován, budou totiž zásahy do zaměstnancova soukromí prováděné ze strany zaměstnavatele legální.

Pokud jde o již naznačenou otázku obsahu informačního sdělení, lze tedy dovozovat, že zaměstnavatel nemusí poskytovat veškeré informace o zamýšleném sledování. Měl by nicméně poskytnout informace alespoň o tom, že sledování bude prováděno, jaké prostředky k tomu budou využity, o způsobech kontroly a rámcově určit dobu, kdy bude sledování prováděno. Forma sdělení, jak má zaměstnavatel informovat, rovněž není stanovena. Za nesprávný je potřeba považovat názor, že by informace musely být poskytovány písemně.[286] Jelikož forma není definována, bylo by možné informaci poskytnout i jinou formou, včetně ústního sdělení, vyvěšením informace na (elektronické) nástěnce apod. Na druhou stranu lze obecně doporučit, aby zaměstnavatel byl vždy schopen prokázat, že informační povinnost splnil. Výhradně ústní poskytnutí informací se tak z tohoto hlediska nejeví jako příliš praktické.

---

[283] Srov. ustanovení § 316 odst. 3 ZPr.

[284] Štefko nicméně upozorňuje, že skryté či tajné sledování může být v rozporu s judikaturou ESLP (srov. Štefko, M. *Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochraně lidských práv a základních svobod*. Jurisprudence. 2012, č. 7-8, s. 19).

[285] Štefko, aniž by rozlišoval skryté a otevřené sledování, rovněž uzavírá, že informování zaměstnance musí být splněno předem (Štefko in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1244). Morávek na tento problém u skrytého sledování upozorňuje a dochází k obdobnému závěru jako autor této práce (Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 580).

[286] Např. Štefko in Bělina, M. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. Velké komentáře, s. 1243.

5.4.5 Aplikace ustanovení v praxi

Otázkou dále zůstává, zda se předmětné ustanovení aplikuje rovněž na případy, kdy existuje zvláštní právní předpis, který ukládá (byť ne přímo) zaměstnavatelům příslušné sledování zaměstnanců provádět. Ač půjde spíše o vzácné případy, bude se jednat například o zvlášť specifická odvětví, jako je provoz jaderných elektráren[287] či provoz chemických zařízení.[288] Podle autora této práce by se měla tato pravidla uplatnit i na tyto případy (přinejmenším obdobně). Totiž i v situacích, kdy sledování zaměstnanců je de facto uloženo zákonem, mají tito svá určitá práva a nepochybně budou mít nárok na to, aby byly o takovém sledování řádně informováni ve smyslu § 316 odst. 3 ZPr (výkladem a contrario by totiž bylo možné dovodit, že zaměstnance o sledování ani není nutné informovat).[289]

Ještě důležitější otázkou pro praxi, jelikož dopadá na všechny zaměstnavatele oprávněné sledování provádět, je rozsah či předmět prováděného sledování. Pokud budou u zaměstnavatele dány závažné důvody spočívající ve zvláštní činnosti zaměstnavatele, pokud splní informační povinnost a pokud se skutečně rozhodne sledování zaměstnanců zavést, neplatí, že by sledování mohlo být bezmezné. Výše v bodě 5.4.2 bylo zmíněno, že v rámci testu přiměřenosti bude muset zaměstnavatel posuzovat zájmy zaměstnavatele a zaměstnance a podle toho volit odpovídající prostředek sledování. I při použití takového sledovacího prostředku bude muset nicméně zaměstnavatel šetřit soukromí zaměstnance.

Štefko toto jednoduše vystihuje, když uvádí, že *„prováděním sledovacích opatření nesmí dojít k nepřiměřenému zásahu do soukromí zaměstnance“*.[290] To je obvykle vykládáno zejména tak, že zaměstnavatel při sledování nesmí zpracovávat a uchovávat obsah soukromých zpráv, prohlíženého webu apod. Měl by naopak sledovat pouze skutečnost, že zaměstnanec například nevykonává své pracovní povinnosti, a to podle adres navštívených webových stránek, hlaviček e-mailů apod. K tomuto názoru se kloní judikatura

[287] Povinnosti stanovené vyhláškou č. 361/2016 Sb. o zabezpečení jaderného zařízení a jaderného materiálu.
[288] Povinnosti stanovené vyhláškou č. 225/2015 Sb. o stanovení rozsahu bezpečnostních opatření fyzické ochrany objektu zařazeného do skupiny A nebo skupiny B.
[289] Odlišně Morávek, který pro tyto situace, kdy je kontrola zaměstnanců uložena zvláštním právním předpisem, aplikaci ustanovení § 316 odst. 2 vylučuje (srov. Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 577).
[290] Op. cit. sub. 286.

českých[291] i evropských[292] soudů a obdobně se vyjadřuje též ÚOOÚ.[293] Více k možnostem sledování zaměstnanců je uvedeno v podkapitole 8.1.

Vedle toho by také obecně neměly být sledovací nástroje aplikovány nonstop, ale naopak by k jejich aplikaci mělo docházet pouze nárazově (umožňuje-li to jejich povaha a je-li to dostatečné z hlediska požadovaného cíle). Jen takovýto postup, kdy budou minimalizovány zásahy do soukromí na nejnižší možnou úroveň, bude přípustný. V této souvislosti se nabízí zopakovat, že zaměstnavatelé by měli jednoduše k zavedení sledovacích nástrojů přistupovat jako k poslednímu možnému řešení. Například v případě webových stránek by zaměstnavatel měl primárně zablokovat obsah webových stránek, které by zaměstnanec neměl navštěvovat apod.

5.4.6 Shrnutí

Legislativní úprava kontrolního oprávnění zaměstnavatele dle ustanovení § 316 odst. 1 a 2 ZPr má relativně dost závažných nedostatků. Výše bylo poukázáno, že toto ustanovení nabízí příliš mnoho nejasných otázek, na které existuje příliš mnoho nejasných názorů. I když v rámci daného ustanovení dochází ke střetu dvou či více ústavních práv, které se projevují v zájmu zaměstnance na ochranu soukromí a v zájmech zaměstnavatele (a taková pravidla musí vždy ponechávat určitý prostor pro výklad, aby bylo možné je vyložit s ohledem na konkrétní skutkové okolnosti), musí rovněž taková pravidla poskytovat určitou míru právní jistoty o svém obsahu. S ohledem na rozsáhlost podaného výkladu je zřejmé, že hledání odpovědi na přípustnost zavedení sledovacích opatření nebude nikdy lehká a je nutné zvažovat celou řadu okolností. Trefně ustanovení § 316 ZPr popisuje Morávek, když uvádí, že *„je možné dovodit relativně racionální pravidla regulující určité podstatné momenty vztahu zaměstnance a zaměstnavatele. Cesta, která vede k racionálním závěrům, je však příliš složitá.“*.[294] Bližší pohled autora této práce k možnostem de lege ferenda je nabídnut v podkapitole 9.2.

[291] Skutečnost, že nebyl monitorován obsah e-mailových a jiných zpráv, byla hodnocena též v již citovaném rozhodnutí Nejvyššího soudu sp. zn. 21 Cdo 1771/2011.
[292] Srov. zejména rozhodnutí ESLP v podkapitole 3.3 a 3.4.
[293] Srov. stanovisko ÚOOÚ č. 2/2009: *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*. Únor 2009.
[294] Morávek, J. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), s. 581.

5.5 Chráněné zájmy zaměstnavatele

Výklad o kontrolních oprávněních zaměstnavatele a jeho zásazích do soukromí zaměstnanců by byl neúplný, pokud by problematika kontrol a sledování nebyla analyzována též z pohledu zaměstnavatele. Jde tedy o analýzu toho, co opravňuje zaměstnavatele do soukromí zaměstnanců zasahovat, resp. jaké jeho zájmy jsou natolik významné, že v rámci testu proporcionality převáží nad právem na ochranu osobnosti a soukromí zaměstnanců. Primárním a nejčastěji v této práci zmiňovaným důvodem či zájmem zaměstnavatele je ochrana jeho majetku.[295] To však rozhodně není jediný důvod, proč zaměstnavatel své zaměstnance kontroluje. Na druhou stranu platí, že v podstatě veškeré dále zmíněné důvody mají přímý či nepřímý vliv na majetek zaměstnavatele.

Vedle ochrany majetku se může jednat též o ochranu obchodního tajemství či know-how zaměstnavatele, byť tyto skutečnosti s ochranou majetku úzce souvisí, neboť jejich porušení by mělo negativní dopad na majetek zaměstnavatele. Zaměstnavatel má rovněž nepochybně právo kontrolovat zaměstnance s ohledem na plnění jejich pracovních povinností, byť i v tomto případě jsou kontroly či sledování zaměstnanců úzce spjaty s ochranou majetku zaměstnavatele, neboť zaměstnanec neplnící své pracovní povinnosti zaměstnavateli nevydělává a ten mu bezdůvodně vyplácí mzdu. V těchto případech se lze již odkázat na konkrétní zákonná oprávnění,[296] která díky svému explicitnímu zákonnému zakotvení dávají zaměstnavateli pádnější důvody pro zavedení kontrolních či sledovacích opatření.[297]

Je zřejmé, že zaměstnavatel ve své roli nemůže být jen pasivní. ZPr mu ukládá celou řadu povinností, které mohou vést k oprávnění zaměstnavatele zavést určité kontrolní či sledovací mechanismy. Při jejich nezavedení by pak zaměstnavatel neplnil své povinnosti a vystavoval by se riziku sankce ze strany dozorového orgánu a případnému riziku spočívajícímu v povinnosti nahradit zaměstnancům vzniklou škodu. Zde je tedy možné důvod pro zavedení daných mechanismů zaměstnavatele vymezit jako zájem na plnění

[295] O ochraně majetku bylo pojednáno především při výkladu o ustanovení § 316 odst. 1 ZPr (srov. podkapitola 5.3), nicméně platí, že ochrana majetku je relevantní i v jiných situacích využití kontrolních a sledovacích prostředků, a proto je relevantní též výklad podaný v jiných podkapitolách této kapitoly.

[296] Jde zejména o povinnosti zaměstnanců dle § 301 ZPr, jejichž dodržování je zaměstnavatel oprávněn vyžadovat a přiměřeně kontrolovat.

[297] V této souvislosti mohou být obdobný, byť méně významný, účinek též interní předpisy zaměstnavatele stanovící bližší povinnosti zaměstnanců, včetně povinnosti nadřízených zaměstnanců podřízené zaměstnance kontrolovat.

zákonem uložených povinností. Asi nejobjemnější povinnosti jsou zaměstnavateli z tohoto pohledu uloženy v souvislosti s BOZP.

Pravidla BOZP jsou v rámci ZPr obsaženy v ustanovení § 101 a násl. a zaměstnavatel je podle nich povinen zajistit bezpečnost a ochranu zdraví zaměstnanců při práci s ohledem na rizika možného ohrožení jejich života a zdraví, která se týkají výkonu práce.[298] Z hlediska možného, byť nikoliv přímého sledování zaměstnanců stojí za zmínku především povinnost vyjádřená v ustanovení § 102 odst. 3 ZPr, podle kterého platí, že *„zaměstnavatel je povinen soustavně vyhledávat nebezpečné činitele a procesy pracovního prostředí a pracovních podmínek, zjišťovat jejich příčiny a zdroje. Na základě tohoto zjištění vyhledávat a hodnotit rizika a přijímat opatření k jejich odstranění a provádět taková opatření, aby v důsledku příznivějších pracovních podmínek a úrovně rozhodujících faktorů práce dosud zařazené podle zvláštního právního předpisu jako rizikové mohly být zařazeny do kategorie nižší. […].“*. V rámci tohoto ustanovení tedy zákonodárce dokonce zaměstnavateli ukládá určitou soustavnou kontrolu pracoviště provádět. Ač je zřejmé, že předmětem takových kontrol nemá být pracovní výkonnost zaměstnance či ochrana majetku zaměstnavatele, je nepochybné, že tyto skutečnosti můžou a mnohdy budou nepřímým produktem takových soustavných vyhledávacích činností zaměstnavatele.

Obdobně pokud jde o povinnosti náhrady majetkové a nemajetkové újmy, je zaměstnavateli v rámci § 248 odst. 1 ZPr uloženo *„zajišťovat svým zaměstnancům takové pracovní podmínky, aby mohli řádně plnit své pracovní úkoly bez ohrožení zdraví a majetku; zjistí-li závady, je povinen učinit opatření k jejich odstranění“*. Nepochybně by bylo možné dohledat též další konkrétní povinnosti stanovené zaměstnavateli na zákonné i podzákonné úrovni (například v rámci nařízení vlády č. 361/2007 Sb.), to však není záměrem. Tím bylo jen poukázat na existenci těchto povinností.

5.5.1 Odpovědnost zaměstnavatele za jednání zaměstnance

Důležitou otázkou, která rovněž do značné míry odůvodňuje zavedení kontrolních a sledovacích mechanismů, je otázka odpovědnosti. Může jít o odpovědnost soukromoprávní i veřejnoprávní. Z hlediska soukromoprávní odpovědnosti je důležité zejména ustanovení § 167 ObčZ,[299] přiznávající zaměstnavateli (je-li jím právnická

[298] Srov. ustanovení § 101 odst. 1 ZPr.
[299] Podle tohoto ustanovení platí, že *„právnickou osobu zavazuje protiprávní čin, kterého se při plnění svých úkolů dopustil člen voleného orgánu, zaměstnanec nebo jiný její zástupce vůči třetí osobě“*.

osoba)[300] odpovědnost za protiprávní čin zaměstnanců, jehož se dopustili v souvislosti se zaměstnáním.

Pokud jde o veřejnoprávní odpovědnost, je třeba rozlišovat odpovědnost za přestupky a trestněprávní odpovědnost (ačkoliv závěry jsou velmi podobné). Odpovědnost za přestupky je upravena v zákoně č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů (dále jen „PřesZ"). Podle tohoto zákona platí, že právnická osoba (zaměstnavatel) bude považována za pachatele, způsobila-li přestupek osoba, jejíž jednání je právnické osobě přičitatelné. Zároveň je též samozřejmě nutné, aby toto jednání bylo v přímé souvislosti s činností právnické osoby.[301] Pokud jde o zmíněný koncept přičitatelnosti, je zároveň stanoveno najisto, že jednání zaměstnance či osoby v obdobném postavení je přičitatelné právnické osobě.[302]

Z hlediska oprávnění zaměstnavatele provádět kontroly je pak významné, že odpovědnost právnické osoby za spáchaný přestupek je založena na konceptu objektivní odpovědnosti. Z toho je nicméně umožněna liberace, avšak pouze za podmínek ustanovení § 21 PřesZ. Podle ustanovení § 21 odst. 2 PřesZ přitom platí, že *„právnická osoba se nemůže odpovědnosti za přestupek zprostit, jestliže z její strany nebyla vykonávána povinná nebo potřebná kontrola nad fyzickou osobou, která se za účelem posuzování odpovědnosti právnické osoby za přestupek považuje za osobu, jejíž jednání je přičitatelné právnické osobě, nebo nebyla učiněna nezbytná opatření k zamezení nebo odvrácení přestupku"*. Toto ustanovení je z hlediska ochrany soukromí (nejen) zaměstnanců relativně problematické, neboť neobsahuje žádný korektiv, který by výkon kontrol omezoval, zákon potřebnost kontrol nijak nespecifikuje a ustanovení o vyloučení odpovědnosti bývají vykládána obvykle spíše restriktivně.[303] Navíc se pro úspěšnou liberaci vždy musí prokazovat vynaložení veškerého úsilí, které je možné objektivně požadovat, aby přestupku bylo zabráněno.[304]

---

[300] Obdobná odpovědnost se však uplatní i na fyzické osoby zaměstnavatele, a to s odkazem na ustanovení § 2914 ObčZ.
[301] Srov. ustanovení § 20 odst. 1 PřesZ.
[302] Srov. ustanovení § 20 odst. 2 písm. c) PřesZ.
[303] Srov. například závěry Nejvyššího správního soudu ČR v rozhodnutí ze dne 14. srpna 2015, sp. zn. 5 As 10/2015, v rámci kterého soud dovodil: *„Připuštěním navrhovaných liberačních důvodů (zabezpečení povinného školení řidičů) by mohlo být liberační ustanovení aplikováno ve velkém množství případů, a ztratilo by tak povahu výjimky z obecného pravidla, což by znamenalo ohrožení veřejného zájmu."*
[304] Srov. ustanovení § 21 odst. 1 PřestZ. Judikatura tento požadavek vykládá tak, že právnická osoba musí prokazovat, že *„provedl[a] technicky možná opatření způsobilá účinně zabránit porušování zákona […]. Nepostačí poukaz […]na to, že tato technicky možná opatření po [ní] nebylo možno spravedlivě požadovat, protože by jejich provádění nebylo ekonomické"* (viz rozhodnutí Nejvyššího správního soudu ČR ze dne 19. září 2014, sp. zn. 4 As 123/2014).

Mates k této potřebnosti kontrol uvádí: *„Jaká je míra potřebnosti kontroly, závisí na tom, o jakou činnost se jedná, což lze obdobně říci o nezbytných opatření, jejichž povaha a rozsah jsou závislé na povaze činnosti, o níž jde, zejména s ohledem na možné nebezpečí, které může vyvolat.“*[305] Tím v podstatě dovozuje, že ne vždy je nutné zavádět ty nejpřísnější kontrolní mechanismy. Autor této práce se nicméně domnívá, že je nutné jít ještě dále a je potřebné plně aplikovat ustanovení § 316 ZPr, pokud jde o ochranu soukromí zaměstnance. Bohužel lze konstatovat, že nalezení průniku těchto povinností nebude rozhodně jednoduché. Nicméně při dodržení pravidel popsaných dále v podkapitole 8.1 by to mělo být možné.

S odpovědností za přestupky si je do určité míry podobná trestněprávní odpovědnost podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů (dále jen „TOPO“). I v tomto případě je odpovědnost právnické osoby založena na přičitatelnosti jednání jiných osob, včetně zaměstnanců právnické osoby.[306] Odpovědnost trestněprávní je však založena na zavinění (subjektivní odpovědnost),[307] které je odvozováno od fyzické osoby, která jednání spáchala (tedy v uvažovaném případě zaměstnance), a to v souvislosti s činností právnické osoby. Pokud jde o přičitatelnost, u ní obdobně jako v případě přestupků platí, že jednání bude přičitatelné právnickým osobám, které *„neprovedly taková opatření, která měly provést podle jiného právního předpisu nebo která po nich lze spravedlivě požadovat, zejména neprovedly povinnou nebo potřebnou kontrolu nad činností zaměstnanců nebo jiných osob, jimž jsou nadřízeny, anebo neučinily nezbytná opatření k zamezení nebo odvrácení následků spáchaného trestného činu“*.[308]

I zde se tudíž dovozuje odpovědnost právnické osoby (zaměstnavatele) pro případ, že nebyly řádně vykonávány povinné či potřebné kontroly nad činností zaměstnanců, neplatilo by to jen tehdy, když by dané kontroly nebylo spravedlivé po zaměstnavateli požadovat.[309] Obdobně i zde tudíž není uveden žádný korektiv ochrany soukromí zaměstnance a ten je nutné dovozovat v potřebnosti aplikace § 316 ZPr, případně obecných

---

[305] Mates, P. *Nad některými oblastmi nového zákona o odpovědnosti za přestupky a řízení o nich.* Bulletin advokacie. 2016. č. 12, s. 26.
[306] Srov. ustanovení § 8 TOPO.
[307] Šámal a Dědič in Šámal, P. *Trestní odpovědnost právnických osob: komentář.* 2. vydání. V Praze: C. H. Beck, 2018, s. 176.
[308] Srov. ustanovení § 8 odst. 2 písm. b) TOPO.
[309] Vedle toho se má právnická osoba možnost zprostit odpovědnosti rovněž pokud prokáže, že vynaložila veškeré úsilí, které na ní bylo možno spravedlivě požadovat, aby spáchání protiprávního činu zabránila (srov. ustanovení § 8 odst. 5 TOPO).

ustanovení o ochraně osobnosti. V porovnání s tím jsou však zřejmé vysoké požadavky kladené na zaměstnavatele, aby zaměstnance kontrolovali. Je proto běžné, že velké společnosti mají vydané nejrůznější vnitřní předpisy, etické kodexy a jiné dokumenty, které takové kontroly obsahují, případně mají implementovány nejrůznější kontrolní a sledovací mechanismy, aby se své případné odpovědnosti vyvarovaly. Vyvažovat tyto zájmy s právem zaměstnanců na ochranu soukromí se pak v mnohých případech jeví jako nadlidský úkol. Na ochranu soukromí zaměstnanců však nelze rezignovat. Jde o rovnocenné lidské právo, jehož význam je v pracovněprávních vztazích zdůrazněn slabším postavením zaměstnance.

III. ČÁST OCHRANA OSOBNÍCH ÚDAJŮ ZAMĚSTNANCŮ

6 Východiska a právní základy zpracování osobních údajů

Obsahem třetí části této práce je komplexní analýza pravidel ochrany osobních údajů zaměstnanců, a to nezávisle na pravidlech upravujících ochranu osobnosti a ochranu soukromí. V kapitolách 6 a 7 je detailně analyzováno nařízení GDPR ve vztahu ke zpracování osobních údajů zaměstnanců, postupně podle jednotlivých zásad stanovených tímto nařízením. Právní úprava ochrany osobních údajů je oproti právní úpravě ochrany osobnosti mnohem snáze uchopitelná díky existenci velkého rozsahu pravidel, která je nutno dodržovat. Tato pravidla jsou vyjádřena především v rámci nařízení GDPR, nicméně některá pravidla je nutné hledat též v jiných právních normách, jak bude vysvětleno. Význam pro aplikaci mohou mít též stanoviska dozorových a jiných orgánů a soft law výkladové dokumenty, především výkladová stanoviska WP29 či Evropského sboru pro ochranu osobních údajů. GDPR je, jak z jeho názvu vyplývá, obecným nařízením o ochraně osobních údajů. Proto se samozřejmě neuplatní jen na zpracování osobních údajů zaměstnanců, ale veškerých fyzických osob, například zákazníků, dodavatelů apod. Právě tato skutečnost, že se jedná o obecnou normu, v sobě může skrývat určité výkladové nejasnosti pro zpracování osobních údajů zaměstnanců. Hlavním cílem této kapitoly je proto na takovéto nejasnosti poukázat, zanalyzovat je a poskytnout na ně vlastní pohled.

V této kapitole je nejprve pojednáno o působnosti nařízení GDPR pro vztahy mezi zaměstnancem a zaměstnavatelem a je stručně vysvětleno chápání souvisejících pojmů definovaných nařízením GDPR. Dále je zkoumána již klíčová otázka pro možnost osobní údaje zpracovávat, kterou je určování právního základu pro zpracování osobních údajů.

6.1 Vymezení působnosti a pojmů

Problematika působnosti a aplikace nařízení GDPR by neměla činit větší obtíže, avšak i v této souvislosti mohou vznikat určité nejasnosti, a proto je záměrem této podkapitoly nalézt na ně odpověď. Větší pozornost je dále věnována definicím a pojmům, které jsou v souvislosti se zpracováním osobních údajů využívány. Jejich správné vymezení a pochopení je klíčové pro porozumění následujícímu výkladu. S ohledem na předmět této

práce se v té souvislosti autor práce zamýšlí nad praktickým významem jednotlivých pojmů v pracovněprávních vztazích.

6.1.1 Působnost

Z hlediska výkladu o působnosti nás pro účely této práce zajímá zejména věcná působnost, která je vymezena v čl. 2 odst. 1 GDPR. V něm se uvádí, že *„toto nařízení 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“*. S ohledem na takto široce vymezenou působnost bude prakticky veškeré zpracování osobních údajů zaměstnanců prováděné zaměstnavatelem, resp. jeho zaměstnanci při výkonu práce spadat do působnosti tohoto nařízení. Automatizované zpracování si lze snadno představit jako zpracování dat obsahující osobní údajů v nejrůznějších systémech, naopak neautomatizované zpracování (které by bylo možné označit za manuální) bude obvykle prováděno zaměstnancem bez využití technických prostředků, které by takové zpracování umožňovaly.

V případě neautomatizovaného zpracování je ještě nicméně nutné, aby byla splněna podmínka toho, že údaje jsou nebo mají být zařazeny do určité evidence.[310] Evidencí je v tomto případě toto (neautomatizované) zpracování připodobněno automatizovanému zpracování, kdy je řazení do nějaké evidence prováděno v podstatě vždy. K otázce, jak nahlížet na tuto působnost, se vyjádřil již SDEU, který vyslovil, že *„úkon, který spočívá v tom, že se na internetové stránce odkáže na různé osoby, které jsou identifikovány buď svým jménem, nebo jinými prostředky, například telefonním číslem nebo údaji o pracovních poměrech a zálibách, je ‚zcela nebo částečně automatizovaným zpracováním osobních údajů‘ […]“*.[311] Soud tak dal jasně najevo, že takovouto běžnou činnost, která by se mohla na první pohled jevit jako nahodilá,[312] je nutné považovat za zpracování osobních údajů.

---

[310] Evidencí se dle čl. 4 bodu 6) nařízení GDPR rozumí *„jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska“*.

[311] Srov. rozhodnutí SDEU ze dne 6. listopadu 2003, C-101/01, ve věci Bodil Lindqvist. A ač se tento výklad týkal Směrnice, je plně použitelný na poměry podle nařízení GDPR s ohledem na to, že působnost Směrnice a nařízení GDPR byla v tomto ohledu vymezena v podstatě totožně.

[312] Nahodilé zpracování bylo dříve explicitně vyjmuto z působnosti ZOOÚ v rámci § 3 odst. 4, a to aniž by toto bylo požadováno Směrnicí. Ani nařízení GDPR pak přirozeně tuto výjimku ze své působnosti neobsahuje. I bez toho lze nicméně souhlasit s Nulíčkem, že nahodilé, tj. neúmyslné získání údajů, které nebudou dále zpracovávány, bude i nadále mimo tuto působnost (srov. Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 66).

Mimo věcnou působnost, tedy za činnost, která nebude považována za zpracování osobních údajů zaměstnance, by nicméně podle názoru autora této práce mělo být považováno, pokud například zaměstnanec zašle či jinak sdělí zaměstnavateli nějaké své osobní údaje, aniž by je zaměstnavatel vyžadoval a měl záměr je jakkoliv dále zpracovávat, respektive by je bez prodlení vymazal či jinak odstranil. Ač je za zpracování ve smyslu definice obsažené v nařízení GDPR (viz dále) považováno již pouhé „nahlédnutí" či „výmaz", v tomto případě chybí jakýkoliv záměr dané údaje zařazovat do evidence (byť by k jejich zpracování mohlo dojít i automatizovaně), a proto dle názoru autora této práce není namístě na takové nevyžádané a odstraněné údaje aplikovat ochranu dle nařízení GDPR.

Pro úplnost je ještě vhodné zastavit se krátce nad výlukami z působnosti nařízení GDPR obsaženými v čl. 2 odst. 2. Nabízí se totiž otázka, zda je nutné za zpracování osobních údajů považovat též zpracování osobních údajů prováděné na základě využití svěřených pracovních prostředků, které nesouvisí s plněním pracovních povinností, tj. zpracování není vykonáváno pro zaměstnavatele. Zaměstnavatel takové využití svěřených prostředků, kdy bude docházet ke zpracování osobních údajů, může zaměstnancům nepochybně dovolovat či tolerovat. Jako vhodný příklad se nabízí například využití služebního telefonu, který zaměstnanec využívá tak, že do paměti ukládá své soukromé kontakty a informace o nich, může jít ale i o soukromé e-maily, které zaměstnanec odesílá z pracovního e-mailu. V této souvislosti lze podle názoru autora této práce uzavřít, že se jedná o osobní zpracování prováděné zaměstnancem pro jeho osobní činnosti[313] ve smyslu čl. 2 odst. 2 písm. c) GDPR.[314]

6.1.2 Pojmy

Lze konstatovat, že definování používaných pojmů bývá obecně znakem kvalitně zpracované právní normy, neboť pomocí tohoto přístupu se snižují interpretační obtíže takové předpisu. Obecně platí, že takovýto přístup je více než obvyklý pro evropské normy. A nejinak je tomu u nařízení GDPR. To v čl. 4 poměrně jasně definuje téměř 30 pojmů, které jsou v něm používány. I přes tento přístup nemusí být vždy výklad všech pojmů jednoznačný, a proto je v tomto bodě podán výklad o těch nejdůležitějších, a to ve vztahu k pracovnímu prostředí.

---

[313] Blíže je tento pojem vysvětlen v preambuli (18) nařízení GDPR.

[314] Obdobně Foldová k působnosti ZOOÚ a pojmu osobní potřeba podle § 3 odst. 3 ZOOÚ (Foldová in Kučerová, A. *Zákon o ochraně osobních údajů: komentář*. Praha: C. H. Beck, 2012, s. 18 a násl.).

O skutečnosti, že subjektem údajů je fyzická osoba, není příliš pochyb. V posuzovaném případě půjde tedy o veškeré zaměstnance, jelikož zaměstnanci mohou být jen fyzické osoby. Pro úplnost lze tedy uvést, že subjekty údajů budou též členové orgánů zaměstnavatele, kteří jsou fyzickými osobami, a na ně se celá řada podaných závěrů uplatní obdobně. Jelikož zaměstnavatelem může být též fyzická osoba, i takový zaměstnavatel bude subjektem údajů ve smyslu nařízení GDPR, ale zpracování osobních údajů zaměstnavatele není předmětem této práce.

O mnoho důležitější a obtížněji vyložitelný je pojem osobní údaje. Nařízení GDPR osobní údaje definuje v čl. 4 bodu 1) jako *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě […]; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*. Z podané definice je zřejmé, že osobními údajem nejsou jen identifikační údaje, jak se mnohdy domnívá značná část široké veřejnosti, ale může se jednat v podstatě o neomezené spektrum informací, které je možné vztáhnout k určité fyzické osobě. Z termínu „identifikovatelné“ je dokonce zřejmé, že dotčený subjekt údajů ani nemusí být znám, může existovat pouze možnost (přímá či nepřímá) tuto osobu identifikovat. K takové možné identifikaci přitom může správce využít další informace, které má on sám, které jsou veřejně dostupné nebo které má někdo jiný.

K pojmu osobní údaj se vyjadřují také soudy ve svých rozhodnutích. SDEU například shledal, že osobním údajem je i informace, že se určitá osoba zranila na noze a čerpá částečné volno z důvodu nemoci.[315] Velké publicitě se též dostalo rozhodnutí, podle kterého může být osobním údajem za určitých okolností též IP adresa.[316] Z českých soudů se k věci vyjadřuje nejčastěji Nevyšší správní soud. Ten například ve svém rozhodnutí pod sp. zn. 1 As 113/2012, ze dne 25. února 2015, uzavřel: *„Zákon si […] všímá jenom skutečnosti, zda zaznamenávané údaje lze ztotožnit s konkrétní osobou.“*[317]

Pro úplnost je třeba poznamenat, že ZOOÚ ve znění účinném do 26. července 2004 obsahoval též negativní vymezení osobního údaje, když uváděl: *„O osobní údaj se nejedná,*

[315] Srov. rozhodnutí SDEU ze dne 6. listopadu 2003, C-101/01, ve věci Bodil Lindqvist. V takovém případě se dokonce jedná o zvláštní kategorii osobních údajů. K tomuto pojmu blíže podkapitola 7.4.
[316] Srov. rozhodnutí SDEU ze dne 20. října 2016, C-582/14, ve věci Patrick Breyer vs. Bundesrepublik Deutschland.
[317] Rozhodnutí Nejvyššího správního soudu ČR ze dne 25. února 2015, sp. zn. 1 As 113/2012.

pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků." Toto negativní vymezení však nebylo zcela eurokonformní, a proto bylo v roce 2004 ze ZOOÚ odstraněno. I přesto je tato negativní definice i nadále dovozována. Za zmínku stojí například nedávné rozhodnutí Nejvyššího správního soudu ČR ze dne 20. prosince 2018, sp. zn. 6 As 168/2018, ve kterém soud dospěl k závěru: *„O osobní údaj tedy nepůjde, jestliže s přihlédnutím ke všem prostředkům, které mohou být rozumně použity možnost určení osoby neexistuje nebo je zanedbatelná."*[318] Zejména tedy ze slova „zanedbatelná" je zřejmé, že vztažení informace ke konkrétní osobě není zcela vyloučeno.[319] Takovýto závěr lze jen uvítat, neboť opačný výklad by vedl k neudržitelným závěrům pro výklad ostatních ustanovení nařízení GDPR.[320] Kromě výše zmíněného může být za osobní údaj považováno též například telefonní číslo,[321] a to i přesto, že tento závěr může být jistě diskutabilní (bude vždy záležet na konkrétních skutkových okolnostech, zda bude možné identifikovat určitou osobu, které bude možné se dovolat; obzvláště v případě služebního telefonu obsluhovaného více osobami).

Záměrem však není podat co možná nejobsáhlejší výklad o pojmu osobní údaj, nýbrž poukázat na široký okruh informací, které se za tímto pojmem mohou skrývat. V pracovním prostředí bude snadné si jako osobní údaje představit identifikační a kontaktní údaje zaměstnance, informace o jeho vzdělání, mzdě a jiných benefitech, o pracovní docházce, čerpání dovolené, zákonných odvodech, úrazech, o pracovní výkonnosti a plnění pracovních povinností, jakékoliv informace v osobním spise zaměstnance apod. Někdy může být osobním údajem zaměstnance též informace o určité osobě identifikované pomocí jména (u malého zaměstnavatele, kde je jen jedna osoba takového jména), jindy naopak bude potřeba znát i další informace, aby informace mohla být považována za osobní údaj. Osobními údaji budou též nepochybně veškeré informace získané z kontrol[322] prováděných zaměstnavatelem. U těch už kvalifikace jakožto osobního údaje nemusí být vždy tak zřejmá. Může jít například o tzv. logy (na první pohled bezvýznamné), které mohou svědčit

---

[318] Shodně též výše zmíněné rozhodnutí Nejvyššího správního soudu ČR sp. zn. 1 As 113/2012, nebo rozhodnutí Nejvyššího správního soudu ČR ze dne 17. července 2018, sp. zn. 3 As 3/2017.

[319] Pravděpodobně lze takový výklad shledat správným také s ohledem na nařízení GDPR, které v preambuli (26) uvádí: *„Při určování, zda je fyzická osoba identifikovatelná, by se mělo přihlédnout ke všem prostředkům, jako je například výběr vyčleněním, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby.*" Měřítko „rozumného použití" je tedy použito jako jakýsi korektiv pro definování informace jakožto osobního údaje. Obdobné pravidlo dříve obsahovala také Směrnice ve své preambuli (26).

[320] Například ve vztahu k právu na přístup k osobním údajům; srov. výklad v podkapitole 7.2.

[321] Srov. rozhodnutí Nejvyššího správního soudu ČR ze dne 12. února 2009, sp. zn. 9 As 34/2008.

[322] Ve smyslu kontrolních oprávnění zaměstnavatele, jak o nich byl podán výklad v kapitole 5.

o konkrétním jednání zaměstnance na svěřené výpočetní technice zaměstnavatele.[323] Blíže k možnostem zpracování jednotlivých osobních údajů v rámci pracovněprávního vztahu viz podkapitola 7.3.

Dalším z důležitých pojmů při výkladu o zpracování osobních údajů, je samotný termín „zpracování". Nařízení GDPR podává velmi širokou definici tohoto termínu, shodně jako tomu bylo v rámci Směrnice či ZOOÚ.[324] Za zpracování tedy bude považováno nejen systematizované nakládání s osobními údaji, ale i jednorázové. Zároveň nemají význam prostředky, kterými je zpracování osobních údajů dosahováno. Může se jednat o zpracování manuální či elektronické, může jít o kombinaci těchto možností nebo i o jiné řešení, existuje-li nebo bude-li v budoucnu existovat.

Záměrem opět není podat úplný výklad o tomto pojmu, ale zhodnotit jeho význam s ohledem na předmět této práce. Ve vztazích mezi zaměstnancem a zaměstnavatelem není pochyb, že zpracováním bude jakákoliv činnost zaměstnavatele s osobními údaji zaměstnance, která bude souviset s pracovněprávním vztahem daného zaměstnance. Nemusí jít jen o plnění pracovní smlouvy či plnění zákonných povinností zaměstnavatele, samozřejmě budou zpracováním i zmiňované kontroly zaměstnanců.[325] Jiným příkladem může být i jednorázová činnost zaměstnavatele související s náborem zaměstnance (včetně vyhledávání si informací o zaměstnanci na webu), s ukončením jeho pracovního poměru (včetně případného vedení sporu se zaměstnancem).

Jelikož je definice zpracování opravdu velmi široká a zahrnuje i činnosti, jako je „nahlédnutí" či „výmaz", lze souhlasit s Nulíčkem, že za zpracování by měla být považována jen činnost, kdy zpracování je účel (či předpoklad) dané činnosti. Například tedy, pokud má někdo na starosti výmaz osobních údajů zaměstnanců, o zpracování osobních údajů se jedná. Naopak pokud má někdo za úkol servis technických zařízení, kde bude přístup k osobním

---

[323] Takové logy přitom obvykle nebude možné bez dalšího vztáhnout k zaměstnanci, protože se bude například jednat jen o soubor číslic či písmen, a tyto logy budou dávat smysl až po jejich dešifrování pomocí jiného nástroje.

[324] Zpracováním se podle čl. 4 bodu 2) GDPR rozumí: „*jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.*"

[325] V tomto ohledu je vhodné poznamenat, že pokud budou kontroly prováděny kamerovým systémem, bude se (s ohledem na stanovisko ÚOOÚ č. 1/2006: *Provozování kamerového systému z hlediska zákona o ochraně osobních údajů*. Leden 2006.) za zpracování osobních údajů považovat, pouze pokud bude z kamer pořizován též záznam. V případě, že by kontroly byly pořizovány jen v online režimu, ke zpracování osobních údajů by nedocházelo (i tak však samozřejmě může docházet k neúměrným zásahům do práva zaměstnance na ochranu jeho soukromí).

údajům spíše nahodilý, o zpracování by se jednat nemělo.[326] Opačný závěr by totiž mohl vést k praktické nemožnosti splnění povinností stanovených správcům (ať už jde o povinnost uzavírat smlouvy se zpracovateli, plnit právo na přístup k osobním údajům apod.).

Tím lze plynule navázat na v této práci již často používaný, avšak dosud nevysvětlený pojem, kterým je správce osobních údajů. Tím se rozumí *„fyzická nebo právnická osoba […] nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; […]"*. Správcem je nepochybně ten, kdo za zpracování osobních údajů v plné míře odpovídá,[327] přičemž rozhodné pro jeho definování subjektu jako správce je právě zmíněné určování účelu a prostředků. V pracovněprávní oblasti tak bude správcem osobních údajů zaměstnanců vždy jejich zaměstnavatel, který bude určovat účely zpracování (plnění povinností zaměstnavatele z pracovních smluv či ze zákona, hodnocení zaměstnanců, ochrana majetku zaměstnavatele apod.) a prostředky takového zpracování (IT systémy zaměstnavatele či třetí osoby, osobní spis, manuální či automatizované zpracování ze strany jiných zaměstnanců apod.).

Za zmínku ještě pro úplnost stojí, že zaměstnavatel může být za určitých okolností též společným správcem osobních údajů zaměstnanců s třetí osobou. WP29 například považuje za společné správce zaměstnavatele a personální agenturu, která zajišťuje pro zaměstnavatele nové zaměstnance a přitom čerpá ze své vlastní databáze uchazečů o zaměstnání (aniž by prováděla specifické oslovování na základě pokynů zaměstnavatele a bylo by ji možné považovat za pouhého zpracovatele).[328] Půjde však o spíše specifické případy, které navíc nemají větší význam pro předmět zkoumání v této práci. V této práci je zkoumáno postavení zaměstnavatele jakožto (samostatného) správce osobních údajů, který plně odpovídá za zpracování osobních údajů svých zaměstnanců.

Asi posledním definovaným pojmem, který je vhodné zmínit, je pojem zpracovatel osobních údajů. Za zpracovatele nařízení GDPR označuje fyzickou nebo právnickou osobu, orgán veřejné moci, agenturu nebo jiný subjekt, který zpracovává osobní údaje pro správce.[329] Jedná se tedy o velmi široké vymezení, kde v podstatě jediným určujícím znakem je, že se jedná o zpracování „pro" správce. Zpracovatel tedy nezpracovává osobní údaje ze

---

[326] Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 86.
[327] Srov. čl. 5 bod 2) nařízení GDPR.
[328] Stanovisko WP29 č. 1/2010: Ke konceptům „správce" a „zpracovatel" (v originále: *opinion 1/2010 on the concepts of "controller" and "processor"*). (WP169) ze dne 16. února 2010, s. 19.
[329] Srov. čl. 4 bod 8) nařízení GDPR.

svého vlastního rozhodnutí, ale činí tak v souladu a dle pokynů správce. Vztah mezi správcem a zpracovatelem může být určen zákonem či se může jednat o smluvní vztah mezi těmito dvěma subjekty. Platí také, že zpracovatel se může podílet jen na vybraném úseku zpracování (může například vypočítávat mzdu pro zaměstnance) nebo může de facto provádět veškeré zpracování osobních údajů a role správce se omezí v podstatě jen na určování pokynů pro zpracovatele a nesení primární odpovědnosti za zpracování.

V oblasti pracovněprávních vztahů bude zpracovatelem například personální agentura,[330] která bude na základě pokynů zaměstnavatele vyhledávat nové zaměstnance, může jím být osoba či společnost pověřená zajišťováním výpočtu mzdy a plněním zákonných povinností, může se jednat o bezpečnostní agenturu zajišťující dohled na pracovišti, ale může jít i o nezávislého „mystery shoppera", který bude pro zaměstnavatele smluvně zajišťovat prověřování plnění pracovních povinností ze strany zaměstnanců. Pro úplnost je vhodné uvést, že zpracovatelem nebude personální oddělení zaměstnavatele, protože to nemá vlastní právní osobnost a považuje se za součást zaměstnavatele.

6.2 Zákonnost zpracování a účelové omezení

V této podkapitole jsou do detailu zkoumány jednotlivé právní základy, které opravňují zaměstnavatele osobní údaje zaměstnanců zpracovávat. S tím též úzce souvisí otázka účelů zpracování a zásada účelového omezení,[331] neboť tyto dvě otázky jsou spolu úzce propojeny (právní základ je možné je identifikovat, jen pokud je jasně určen účel zpracování osobních údajů). I účelům zpracování osobních údajů tedy je dále věnována pozornost.

Právní základy pro zpracování osobních údajů vymezuje nařízení GDPR v čl. 6, kde je uvedeno celkem šest různých právních základů. Jednotlivým právním základům, které jsou relevantní pro vztahy mezi zaměstnancem a zaměstnavatelem na pracovišti, se postupně věnují samostatné body této podkapitoly. Využití zbývajících dvou právních základů, tj. ochrana životně důležitých zájmů subjektů údajů a splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, bude spíše okrajové, a proto jim není věnována bližší pozornost.[332]

---

[330] S výjimkou výše zmíněných případů, kdy by ji bylo možné považovat za společného správce.

[331] Tato zásada je v nařízení GDPR definována v tom smyslu, že osobní údaje musí být „*shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný […]*." (srov. čl. 5 bod 1 písm. b) nařízení GDPR).

[332] Využití právního základu „*ochrana životně důležitých zájmů subjektů údajů*" se bude v pracovněprávních vztazích obvykle překrývat s povinnostmi zaměstnavatele na úseku BOZP, a zaměstnavatel proto bude (pro

Mezi jednotlivými právními základy není žádná, předpisy definovaná, chronologie a bylo by možné konstatovat, že všechny jsou si rovnocenné.[333] V praxi a s ohledem na zpracování uložená zákonem toto však zcela neplatí. Předně se s odkazem na stanoviska ÚOOÚ, ale též stanoviska WP29 vyprofiloval závěr, že souhlas není namístě využívat, pokud existuje jiný právní základ. Lze konstatovat, že s ohledem na jeho charakter (odvolatelnost) je tento závěr více než vhodný.[334] Podle názoru autora této práce k tomu lze též dodat, že pokud je souhlas právním základem na posledním místě, měl by být oprávněný zájem na předposledním místě.[335] U právních základů zpracování osobních údajů spočívajících v plnění smlouvy či zákonných povinností není potřebné prioritizaci řešit. Tyto právní základy se mohou navíc v pracovněprávní oblasti ve značné části překrývat, jak bude vysvětleno dále.

Před výkladem o jednotlivých právních základech je ještě nutné věnovat pozornost zásadě účelového omezení, která s právními základy úzce souvisí. Tuto zásadu lze považovat za zásadní pro jakékoliv posuzování přípustnosti či možnosti a zákonnosti a případných jiných otázek zpracování osobních údajů (omezení uložení, minimalizace údajů atd.). Platí totiž, že osobní údaje mohou být zpracovávány jen pro (i) určité, (ii) výslovně vyjádřené a (iii) legitimní účely. Každý správce je proto povinen takovéto účely stanovit ještě před zahájením zpracování, tj. před započetím shromažďování zpracování osobních údajů.[336]

---

v podstatě shodné účely) obvykle povinen osobní údaje zpracovávat, aby dostál svých povinností uložených ZPr. Pokud jde o právní základ „*splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci*“, ten bude mít svůj význam především u subjektů, kterým je ze zákona svěřena určitá působnost v oblasti veřejného zájmu (například subjekty spravující distribuční sítě, subjekty vykonávající komunikační činnosti, správci státních rezerv apod.), nebo u subjektů veřejné správy. I v těchto případech může (pro obdobné účely) zaměstnavatel dovodit i jiný právní základ pro zpracování osobních údajů. Existence tohoto dalšího či jiného právního základu může mít nicméně vliv i na možnost zaměstnavatele zavést určité kontrolní mechanismy. Například u subjektů provádějících činnosti ve veřejném zájmu je obvykle ve vyšší míře obhajitelná ochrana majetku a tím i vyšší míra možnosti zásahů do ochrany soukromé fyzických osob, včetně zaměstnanců.

[333] ZOOÚ sice na první pohled preferoval zpracování osobních údajů založené na souhlasu (srov. ustanovení § 5 odst. 2 ZOOÚ, které uvádělo, že „*správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat […]*“). Ze stanovisek ÚOOÚ však bylo patrné, že takto formulované ustanovení nemělo žádný vliv na skutečnost, že souhlas neměl být preferovaným (spíše až posledním) právní základem pro zpracování osobních údajů (srov. Stanovisko ÚOOÚ č. 3/2014: *K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti*. Srpen 2014).

[334] Blíže viz bod 6.2.4.

[335] Blíže viz bod 6.2.3.

[336] Odlišně Nulíček, který s odkazem na preambuli (39) nařízení GDPR dovozuje, že stanovení účelů musí proběhnout nejpozději „při“ shromažďování osobních údajů (srov. Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 108). Dle názoru autora této práce však takový výklad z dané preambule nevyplývá. Naopak z něj vyplývá, že účely musí být stanoveny již v okamžiku shromažďování.

Všechny tři výše zmíněné požadavky kladené na vymezení účelů mají přitom svůj určitý význam. Pokud jde o požadavek na „určitost" účelů, ten spočívá v tom, aby správce odpověděl na otázku, proč chce nebo musí osobní údaje zpracovávat. Jedná se tedy o interní posouzení údajů prováděné správcem, které je nezbytným předpokladem jeho odpovědnosti za zpracování osobních údajů.[337] Pokud jde o míru určitosti, v jaké by měl být účel zpracování určen, měla by být taková, aby bylo zřejmé, jaké zpracování osobních údajů je ještě možné zahrnout pod tentýž účel a jaké zpracování stojí již mimo něj. Určení účelů by tedy nemělo být příliš vágní, na druhou stranu i příliš konkrétní určení účelů nemusí být ku prospěchu věci, neboť ze zpracování pak mohou vypadnout některé činnosti, které do něj původně zahrnuty být měly. Míra určení detailu se také bude lišit případ od případu s ohledem na ostatní podmínky zpracování, jako je zejména rozsah.[338]

V pracovněprávní oblasti nebude obvykle problém určit účely v situacích, kdy zaměstnavatel bude plnit své zákonné povinnosti. Již poněkud komplikovanější může být situace při plnění povinností dle smlouvy, neboť ve smlouvě mohou být relativně neurčitá ujednání dovolující zaměstnavateli provádět různá hodnocení zaměstnancova výkonu. Na to obdobně plynule navazuje určování účelu pro situace, kdy je právním základem oprávněný zájem zaměstnavatele.[339] Za problematické by například muselo být označení účelu zpracování jako „HR management" nebo „řízení lidských zdrojů", neboť se jedná o velmi široké pojmy, pod kterými si lze představit provádění širokého spektra činností. Naopak za vhodné vymezení účelu by bylo možné považovat „hodnocení výkonu zaměstnance", „administrace a správa pracovněprávního vztahu" nebo „péče o odborný rozvoj zaměstnanců". Takto vymezené účely již nabízejí větší představu o konkrétních vykonávaných činnostech. Samozřejmě platí, že pokud by dříve naznačené nevhodné účely (HR management a řízení lidských zdrojů) byly jen zastřešujícími pojmy a zaměstnavatel by v rámci vrstevnatosti nabízel i jejich bližší specifikaci, byly by podle názoru autora této práce i takto široce vymezené účely připustitelné.

---

[337] Stanovisko WP29 č. 3/2013: K účelovému omezení (v originále: *opinion 3/2013 on purpose limitation*). (WP203), ze dne 2. dubna 2013, s. 15.

[338] Tamtéž, s. 15 a 16. Zmíněné stanovisko WP29 také uvádí, že subjektům údajů by měla být předložená „vrstevnatá" informace o účelech v tom smyslu, že subjekt údajů může být o účelech informován relativně obecněji, pokud však má možnost zájem o bližší informace k takovému vymezení účelu, má mu to být umožněno.

[339] Naopak problém s určitostí účelu by neměl být ani v případě zpracování osobních údajů zaměstnanců založeném na souhlasu s ohledem na omezenou využitelnost tohoto právního základu v pracovněprávních vztazích (blíže viz bod 6.2.4).

Druhým požadavkem na účel je výslovnost jeho vyjádření. Správci osobních údajů tedy nestačí provést jeho jednoznačné určení ve výše uvedeném smyslu, musí jej také explicitně vyjádřit, zachytit a sdělovat jej subjektům údajů. Rovněž by měli správci zajistit, aby explicitně vyjádřený účel byl vykládán všemi dotčenými osobami (správce, zpracovatel, subjekty údajů, dozorový orgán) stejně a neumožňoval různé výklady.[340] Z uvedeného také vyplývá, že požadavek na výslovně vyjádřený účel úzce souvisí se zásadou transparentnosti, která je popisována v následující podkapitole 7.1. Jen při splnění této podmínky nebude správcům umožněno účel přizpůsobovat s ohledem na své aktuální potřeby a bude zajištěna zákonnost zpracování osobních údajů. Pokud jde o vztah zaměstnavatele k tomuto požadavku, plně jej zajistí prostřednictvím zachycení účelu v rámci informačních dokumentů (čl. 13 GDPR) či v rámci zaměstnavatelem povinně vedených záznamech o činnostech zpracování (čl. 30 GDPR).

Poslední, neméně důležitý požadavek na vymezení účelu se týká legitimity účelu. Předně musí být účel vždy spjat s určitým právním základem. Vedle to by měl být též v souladu s obecně závaznými právními předpisy (nejen předpisy týkajícími se ochrany osobních údajů). Není nicméně nutné, aby v nich měl oporu, spíše platí, že s nimi nesmí být v rozporu.[341] Zaměstnavateli tento požadavek nebude z podstaty věci činit žádný problém, pokud bude účel zpracování založen na právním základu plnění zákonných povinností. Obdobně ani u právního základu plnění smlouvy s ním nebude mít zaměstnavatel přílišné potíže, neboť uzavření a plnění pracovní smlouvy je do značné míry regulováno zákonem. Problém tak může nastat u zpracování založených na oprávněném zájmu či na souhlasu zaměstnanců. Teoreticky by si zaměstnavatel mohl definovat účel, jako „kontrola obsahu pošty zaměstnanců“. Takovýto účel by nicméně nepochybně narážel na právo zaměstnanců na ochranu jejich soukromí, proto by nebylo možné jej považovat za legitimní a související zpracování osobních údajů by bylo nezákonné.

6.2.1 Plnění právních povinností

Pokud jde o jednotlivé právní základy, ve vztahu mezi zaměstnancem a zaměstnavatelem je namístě se v první řadě zmínit o splnění právní povinnosti, která se na správce vztahuje ve smyslu čl. 6 odst. 1 písm. c) GDPR. Uzavřením pracovněprávního

[340] Stanovisko WP29 č. 3/2013: K účelovému omezení (v originále: *opinion 3/2013 on purpose limitation).* (WP203), ze dne 2. dubna 2013, s. 17.
[341] Tamtéž s. 20.

vztahu totiž zaměstnavateli vzniká celá řada povinností, které jsou mu uloženy zákonem a z kterých nevyhnutelně vyplývá povinnost zpracovávat osobní údaje zaměstnanců.

Pro úplnost je nutné se věnovat tomuto právnímu základu i teoreticky. Aby bylo možné určitou činnost zpracování osobních údajů provádět s odkazem na plnění právní povinnosti, je nutné, aby existovala povinnost uložená obecně závaznými předpisy (nikoliv například smlouvou)[342] a správce se nemohl dobrovolně rozhodovat, zda ji splní či nikoliv. Pokud by možnost nesplnění byla správci poskytnuta, nepochybně by nešlo o plnění právní povinnosti. Další podmínkou je, aby předmětná právní povinnost byla stanovena dostatečně určitě. Správce by neměl mít možnost volného uvážení o tom, jak právní povinnosti splní. Pokud by výše uvedené podmínky splněny nebyly, není samozřejmě vyloučeno, aby byl správce i tak oprávněn provádět zamýšlené zpracování osobních údajů, pouze však s odkazem na jiný právní základ.[343]

Základními povinnostmi zaměstnavatele jsou ty, které vyplývají přímo ze ZPr. Za zmínku stojí především povinnost zaměstnavatele k vedení evidence odpracované doby (§ 96 ZPr), vedení evidence pracovních úrazů (§ 105 odst. 3 ZPr), vedení osobního spisu (§ 312 ZPr),[344] informační a evidenční povinnosti zaměstnavatele na úseku BOZP (§ 101 a násl. ZPr), vedení evidence svěřených věcí a svěřených hodnot (§ 252 a násl. ZPr), evidence pro potřeby cestovních náhrad (§151 a násl. ZPr), provádění srážek ze mzdy (§ 146 ZPr) apod.

S ohledem na výše podaný výklad ohledně nutnosti jasné a konkrétní zákonem stanovené povinnosti pro využití tohoto právního základu může být poněkud sporné, do jaké míry je plněním zákonné povinnosti poskytování mzdy (či platu nebo odměny) za vykonanou práci ve smyslu § 109 a násl. ZPr, a to s ohledem na skutečnost, že mzda je sjednávána smluvně, nebo bývá stanovena vnitřním předpisem zaměstnavatele. Obdobně výše platu nevyplývá zcela výhradně ze zákona s ohledem na možné nenárokové příspěvky apod. I přesto je podle názoru autora této práce nutné považovat související zpracování osobních údajů za plnění právní povinnosti ze strany zaměstnavatele, a to z toho důvodu, že zaměstnavateli je uložena celá řada (jasně stanovených) navazujících povinností, které by

[342] Pro úplnost lze poznamenat, že se musí jednat o právní předpisy závazné v dané zemi. Nikoliv například v zahraničí.
[343] Stanovisko WP29 č. 6/2014: K pojmu oprávněných zájmů správce podle článku 7 směrnice 95/46/ES (v originále: *opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*). (WP 217), ze dne 9. dubna 2014, s. 19.
[344] Že se jedná o povinnost zaměstnavatele srov. výklad v bodě 4.3.2.

bez zpracování osobních údajů o mzdě zaměstnance nebyl schopen plnit.[345] Nepochybně lze nicméně v tomto případě dovozovat, že zaměstnavatelovo oprávnění ke zpracování osobních údajů o mzdě je nezbytné též pro plnění smlouvy mezi ním a zaměstnancem ve smyslu čl. 6 odst. 1 písm. b) GDPR.[346]

Kromě ZPr existuje celá řada dalších předpisů, které zaměstnavatelům zpracování osobních údajů jejich zaměstnanců ukládají. Za zmínku stojí především povinnosti uložené zákonem č. 48/1997 Sb., o veřejném zdravotním pojištění (povinnost odvádět pojistné dle § 8, oznamovací povinnost dle § 10, využití rodného čísla ve smyslu § 53c), zákonem č. 589/1992 Sb., o pojistném na sociální zabezpečení (odvod pojistného ve smyslu § 8 a násl.), zákonem č. 187/2006 Sb., o nemocenském pojištění (přihlašovací a oznamovací povinnosti ve smyslu § 93 a 94, evidence o zaměstnancích, kteří jsou účastni na pojištění ve smyslu § 95, uchování záznamů podle § 96 apod.), zákonem č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení (povinnost zaměstnavatelů vést záznamy a podávat hlášení pro účely důchodového pojištění ve smyslu § 35a, obsah záznamů dle § 37, evidenční listy dle § 38, hlášení zaměstnávání důchodců dle § 41 apod.), zákonem č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění (stanovení výše pojistného dle § 2 a § 3, odvody pojistného dle § 5), zákonem č. 586/1992 Sb., o daních z příjmů (příjmy ze závislé činnosti dle § 6, slevy na dani dle § 35ba, podávání daňového přiznání dle § 38g, vybírání a placení záloh dle § 38h apod.), zákonem č. 435/2004 Sb., zákon o zaměstnanosti (vedení evidence zaměstnávaných osob se zdravotním postižením a pracovních míst vyhrazených pro osoby se zdravotním postižením ve smyslu § 80), nebo zákonem č. 373/2011 Sb., o specifických zdravotních službách (pracovnělékařské služby a posuzování zdravotní způsobilosti osoby ucházející se o zaměstnání dle § 53 a násl.).

Může se jednat ale také o předpisy upravující povinnosti, které se neuplatní obecně, ale až po splnění dalších podmínek. Obvykle poté, co nastane nějaká právní skutečnost. Příkladem mohou být povinnosti související s prováděním srážek ze mzdy podle zákona č. 120/2001 Sb., exekuční řád (exekuce srážkami ze mzdy a jiných příjmů dle § 60) nebo

[345] Půjde zejména o povinnosti související s oznamováním a ohlašováním příjmů zaměstnanců prováděné zaměstnavateli vůči orgánům sociálního zabezpečení či finančním úřadům apod. (srov. další výklad v této části).

[346] Tato otázka by pravděpodobně mohla vznikat u dalších povinností zaměstnavatele, v rámci kterých není jasně vyjádřena povinnost zaměstnavatele zpracovávat osobní údaje zaměstnanců, ale provádění popisované činnosti k tomu musí nezbytně implikovat (například určité povinnosti na úseku BOZP, povinnosti týkající se odborného rozvoje zaměstnanců ve smyslu § 227 a násl. ZPr či povinnosti vedoucích zaměstnanců ve smyslu § 302 ZPr).

podle zákona č. 99/1963 Sb., občanský soudní řád (srážky ze mzdy podle § 276 a násl.), povinnosti související s platební neschopností zaměstnavatele dle zákona č. 118/2000 Sb., o ochraně zaměstnanců při platební neschopnosti zaměstnavatele a o změně některých zákonů, povinnosti v případě vzniku pracovního úrazu podle nařízení vlády č. 201/2010 Sb., o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu (náležitosti knihy úrazů dle § 2, ohlašovací povinnost a vyhotovení záznamu ve smyslu § 4 a § 5 apod.), podle vyhlášky č. 125/1993 Sb., o zákonném pojištění odpovědnosti zaměstnavatele za škodu při pracovním úrazu nebo nemoci z povolání (součinnost zaměstnavatele dle § 8), nebo související sankční ustanovení podle zákona č. 251/2005 Sb., o inspekci práce (správní delikty dle § 30). Do této kategorie mohou rovněž spadat specifické povinnosti zaměstnavatele dle ZPr. Právní skutečností, která může založit specifické zpracování, může být například skončení pracovního poměru. To samo o sobě nepochybně vyvolá nutnost specifického zpracování osobních údajů (příprava dohody o skončení či výpovědi a uchování těchto dokumentů, příprava potvrzení o zaměstnání). Navíc může být tato skutečnost doprovozena další skutečností, což vyvolá nutnost dalšího zpracování osobních údajů (povinnost zaměstnavatele vydat zaměstnanci pracovní posudek na žádost zaměstnance). Existuje přitom celá řada dalších skutečností, které budou mít za následek (povinné) specifické zpracování osobních údajů (členství zaměstnance v odborech, těhotenství zaměstnankyně, dosažení určitého věku, smrt apod.). Kromě ZPr navíc mohou být tyto povinnosti upraveny i v jiných zvláštních předpisech.[347]

Dále mohou povinnosti zaměstnavatele vyplývat též z řady jiných právních předpisů v závislosti na činnostech zaměstnavatele, a to v tom smyslu, že činnost zaměstnavatele podléhá nějaké specifické regulaci. Příkladem mohou být třeba banky a jiné finanční instituce, na které dopadne plnění povinností dle zákona o bankách (povinnosti související s evidováním střetu zájmů, povinnost postupovat obezřetně a provádět související prověřování zaměstnanců, povinnost zavést mechanismy pro interní hlášení), dále zaměstnavatelé mající povinnosti dle zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (opatření pro hodnocení a identifikaci rizik spočívající v prověřování zaměstnanců, školení zaměstnanců), státní zaměstnavatelé podléhající specifické regulaci dle zákona č. 234/2014 Sb., o státní službě, nebo zaměstnavatelé mající povinnosti zajištění odborného vzdělávání svých zaměstnanců.

[347] Příkladem může být zaměstnávání cizinců, kdy zaměstnavateli vznikají specifické informační povinnosti ve smyslu § 85 a násl. ZoZ.

Výše uvedený přehled lze shrnout v tom smyslu, že existují tři oblasti právních předpisů, ze kterých mohou pramenit povinnosti zaměstnavatelů opravňující je zpracovávat osobní údaje zaměstnanců: (i) právní předpisy aplikující se na všechny zaměstnavatele bez výjimky, (ii) právní předpisy aplikující se na zaměstnavatele, jen v případě nějaké další právní skutečnosti (úraz, smrt, dluh zaměstnance či zaměstnavatele, zaměstnávání cizinců apod.) a (iii) právní předpisy aplikující se v případě, že zaměstnavatel vykonává činnost podléhající zvláštní regulaci. První množina (i) je relativně dobře vymezitelná. U druhé množiny (ii) je to obtížnější s ohledem na v podstatě neomezený počet skutečností, které mohou nastat. Obdobně u třetí množiny (iii) je velmi obtížné vymezit okruh všech potenciálně možných předpisů, které mohou ukládat zaměstnavatelům povinnosti, z nichž bude vyplývat povinnost zpracovávat osobní údaje zaměstnanců. Na druhou stranu platí, že zaměstnavatelé by neměli mít větší problémy s určováním těchto předpisů, neboť se vždy budou s onou specifickou skutečností potýkat, respektive budou vždy řešit jen tu zvláštní regulaci, které budou podléhat.

Závěrem lze konstatovat, že podle názoru autora této práce není příliš rozhodné, do jaké míry detailu bude vymezen účel zpracování osobních údajů související s plněním výše zmíněných povinností.[348] V tomto případě bude nepochybně možné volit relativně obecnější formulace (například, že účelem je *„plnění zákonem stanovených povinností spočívající v…“*), jelikož o rozsahu zpracování osobních údajů skrývajícím se pod takovým účelem by nemělo být větších pochyb. Samozřejmě lze ze strany zaměstnavatelů volit i bližší vymezení účelů jako *„vedení zákonem stanovených evidencí (služební cesty, docházka, svěřené pracovní prostředky, střet zájmů, absolvované školení atd.)“, „plnění zákonných ohlašovacích a oznamovacích povinností“, „vedení mzdové agendy“* apod.

6.2.2 Plnění smluvního vztahu

Druhým právním základem, který je třeba analyzovat, je nezbytnost zpracování osobních údajů pro splnění smlouvy ve smyslu čl. 6 odst. 1 písm. b) GDPR. Ve vztahu mezi zaměstnancem a zaměstnavatelem se bude tedy jednat o uzavření pracovní smlouvy či některé z dohod o pracích konaných mimo pracovní poměr. Nemusí se však vždy jednat jen o tyto případy smluv či dohod. Ve vztahu mezi zaměstnancem a zaměstnavatelem se může jednat též o zpracování údajů související s uzavřením dohody o odpovědnosti za svěřené

[348] Srov. výše zmíněné požadavky na určitost, explicitní vyjádření a legitimitu účelů (srov. výklad výše v podkapitole 6.2).

hodnoty, dohody o odpovědnosti za ztrátu svěřených věcí, kvalifikační dohody, dohody o dočasném přidělení apod. Tento právní základ má v pracovněprávních vztazích význam dále též pro nábor zaměstnanců. Aby se tento právní základ mohl aplikovat, není totiž nutnou podmínkou, aby došlo k založení pracovněprávního vztahu smlouvou, neboť ustanovení čl. 6 odst. 1 písm. b) GDPR rovněž uvádí, že zpracování údajů je možné i pro *„provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů“*.[349]

Obsahem tohoto právního základu je v rámci pracovněprávních vztahů zpracování především základních identifikačních údajů zaměstnance, jeho kontaktních údajů, údajů nezbytných pro výplatu mzdy (zejména číslo bankovního účtu) a jiných údajů, jejichž zpracování je nezbytné pro plnění smlouvy. Rozsah zpracovávaných osobních údajů tedy vždy musí vyplývat ze smlouvy a být v souladu se zmíněným korektivem „nezbytnosti“ pro plnění smlouvy. Nemělo by se již jednat o zpracování, které je prováděno na základě jednostranného rozhodnutí či svévole zaměstnavatele. Pro správné určení toho, kdy je ještě zpracování osobních údajů možné považovat za nezbytné pro plnění smlouvy, je potřeba vycházet ze smyslu, podstaty a účelu uzavření smlouvy jako takové.[350]

V některých případech může být nicméně posouzení nezbytnosti pro splnění smlouvy sporné a může docházet k určitým překryvům s jinými právními základy. Jak bylo naznačeno v předchozím bodě 6.2.1, může se jednat o určitý překryv s plněním právních povinností, kdy například poskytování a výpočet mzdy bude vyplývat jak ze zákona, tak i ze samotné smlouvy. Může se jednat o překryv i s jiným právními základy. Například při vytváření interního telefonního seznamu zaměstnanců, který bude obsahovat jména, zařazení a telefonní čísla a prostřednictvím kterého se budou moci zaměstnanci vzájemně kontaktovat, se může jednat o zpracování nezbytné pro plnění smlouvy (předpokládá-li to smlouva nebo to vyplývá z jejich ustanovení) a může se jednat též o zpracování prováděné s odkazem na oprávněný zájem zaměstnavatele. Naopak nebude pochyb, že u kontrol a sledování zaměstnanců prováděných ze strany zaměstnavatele nebude možné tento právní základ dovodit a v takových situacích bude nutné hledat jiný právní základ (ať už plnění právní povinnosti, či oprávněný zájem zaměstnavatele). Zpracování osobních údajů z důvodu vedení sporu se zaměstnancem, které sice souvisí s existencí smluvního vztahu,

---

[349] Více k možnosti zaměstnavatele zpracovávat osobní údaje zaměstnanců před vznikem pracovněprávního vztahu srov. bod 6.2.4 (a).

[350] Stanovisko WP29 č. 6/2014: K pojmu oprávněných zájmů správce podle článku 7 směrnice 95/46/ES (v originále: *opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*). (WP 217), ze dne 9. dubna 2014, s. 16 a 17.

ale již není vázáno na existenci a plnění smluvního vztahu, bude také mimo rámec tohoto právního základu (snad by za plnění smlouvy bylo možné považovat ještě zaslání upomínek na plnění, ale už by se nejednalo o situace, kdy bude nutné podniknout další kroky, včetně zapojení třetích osob).[351]

Při hledání účelů a rozsahu možného zpracování s odkazem na právní základ plnění smlouvy je rovněž nutné brát v potaz limity stanovené zákony, především ZPr, které do značné míry určují, co smí a nesmí být obsahem těchto smluv. Předně nebude možné ujednat smluvní pokuty (s výjimkou smluvní pokuty související s konkurenční doložkou), nebude možné zástavním právem zajistit budoucí dluh zaměstnavatele vůči zaměstnanci,[352] není možné sjednat zkušební dobu nad zákonný limit,[353] je nutné dodržet pravidla o minimální a zaručené mzdě[354] apod.

Pokud jde o vymezení účelů zpracování odpovídajících tomuto právnímu základu, přiléhavé bude zdůraznit, že zpracování osobních údajů souvisí s plněním pracovní smlouvy, například že účelem je správa a vedení pracovněprávního vztahu na základě pracovní smlouvy. Opět by bylo možné definovat účel i podrobněji (např. evidence související s výplatnou mzdy, poskytování příspěvků a jiných benefitů dle pracovní smlouvy, evidování dovolené), ale ani v tomto případě by neměly vznikat větší pochybnosti o tom, co bude předmětem zpracování, a proto to podle názoru autora této práce není nutné.

6.2.3 Oprávněný zájem

Do jisté míry kontroverzním právním základem pro zpracování osobních údajů je situace, kdy je zpracování ve smyslu čl. 6 odst. 1 písm. f) GDPR nezbytné pro *„účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě“*. Při extenzivním výkladu by se dalo dovozovat, že v podstatě veškeré zpracování osobních údajů prováděné správcem je jeho oprávněný zájem (ať už jsou pohnutky správce jakékoliv, má vždy dobrý důvod, obvykle ekonomický, proč zpracování provádí). Právě z toho důvodu je v rámci nařízení GDPR[355] zakotven korektiv, který tyto oprávněné zájmy či pohnutky správce staví do

[351] Tamtéž s. 17.
[352] Srov. § 346d ZPr.
[353] Srov. § 35 ZPr.
[354] Srov. § 111 a násl. Zpr.
[355] Nejinak tomu bylo v předchozí právní úpravě v rámci § 5 odst. 2 písm. f) ZOOÚ.

protikladu se základními právy a svobodami subjektu údajů, zejména s právem na ochranu soukromí.

Na oprávněný zájem správce (či třetí osoby[356]) jako takový je přirozeně kladeno hodně požadavků. Sice se jedná o odlišný koncept od „účelu“ zpracování, ale do značné míry je možné jej připodobnit. Jde totiž o širší koncept, který v sobě musí zahrnovat i onen později definovaný účel. Proto je zřejmé, že také oprávněný zájem musí být jasně vyjádřen. Vedle toho platí, že musí být skutečný, nikoliv příliš vágní či spekulativní.[357] I pro zájem, obdobně jako pro účel, platí, že musí být legitimní v tom smyslu, že nesmí odporovat právním předpisům, včetně pracovněprávních předpisů a příslušných pravidel upravujících ochranu soukromí zaměstnanců.

Klíčovou je však otázka, co činí zájem oprávněným či neoprávněným. Může se jednat o celou řadu zájmů, které lze jen těžko předem vymezovat.[358] Ve vztahu na pracovišti lze však přece jen tento okruh omezit. Bližší výklad k této otázce byl již podán v podkapitole 5.5. Bude se jednat především o ochranu majetku zaměstnavatele, včetně kontroly využívání svěřených prostředků, kontrolu plnění pracovních povinností zaměstnanců, předcházení podvodům, monitoring bezpečnosti apod. Samozřejmě platí, že tento zájem musí být dostatečně „silný“, aby byl schopen v rámci balančního testu převážit nad základními právy a svobodami zaměstnanců.

Zmiňovaný balanční test je proces, v rámci kterého jsou hodnocena jednotlivá práva a je poměřováno, které právo převažuje, aby bylo zhodnoceno, zda je možné zpracování osobních údajů s odkazem na oprávněný zájem provádět či nikoliv. Nejedná se o formalizovaný proces, který by bylo vždy nutné provádět podle přesných pravidel. Podle názoru autora této práce bude tento proces většinou probíhat jen při úvaze příslušných správců rozhodujících o zahájení zpracování. To bude obvykle možné považovat za dostatečné u jednodušších případů zpracování osobních údajů. Ve složitějších případech (zejména pokud má dojít ke zpracování většího rozsahu údajů či zvláštní kategorie osobních

---

[356] Ačkoliv oprávněný zájem na zpracování osobních údajů může správce dovozovat též u třetí osoby, s ohledem na zaměření této práce, kdy je relevantní zkoumání vztahu zaměstnavatele jako správce a zaměstnance jako dotčeného subjektu údajů, není této otázce věnována bližší pozornost.

[357] Stanovisko WP29 č. 6/2014: K pojmu oprávněných zájmů správce podle článku 7 směrnice 95/46/ES (v originále: *opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*). (WP 217), ze dne 9. dubna 2014, s. 24.

[358] Nulíček v této souvislosti obecně dělí jednotlivé zájmy podle jejich váhy do tří skupin, a to (i) zájmy vyplývající ze základních práv, (ii) veřejné zájmy a (iii) veškeré ostatní zájmy (srov. Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 136).

údajů, výsledek balančního testu by měl být spornější, bude závažněji zasahováno do práv subjektů údajů) by však správce měl vždy, s ohledem na princip odpovědnosti, přistoupit k formálnímu vyhotovení takového balančního testu.

Provádění takového balančního testu totiž mnohdy nebude jednoduchá úloha, v rámci které by se porovnávaly dvě srovnatelné hodnoty, ale většinou půjde o komplexní hodnocení, v jehož rámci bude nutné uvažovat celou řadu faktorů. Jak by se v takovém případě mělo postupovat, nabízí WP29 ve svém stanovisku.[359] Již bylo uvedeno výše, že správce bude muset v první řadě jasně vymezit oprávněný zájem, na který bude při provádění zpracování osobních údajů odkazováno. Druhým krokem je určení toho, zda je zpracování osobních údajů skutečně nezbytné pro dosažení požadovaného zájmu a zda jej nelze dosáhnout i bez zamýšleného zpracování osobních údajů. V té souvislosti tedy správce musí posoudit, zda neexistují nějaké jiné, méně invazivní prostředky, kterými by dosáhl stanovených účelů, resp. by naplnil svůj sledovaný zájem. [360]

Dále by mělo již dojít k samotnému balancování, při kterém by měl správce posuzovat, zda převyšuje jeho oprávněný zájem základní práva a svobody subjektu údajů. V rámci toho by měl především (i) uvážit, v čem spočívá jeho oprávněný zájem (zda jde o základní či jiné právo, zda lze dovozovat veřejný zájem), (ii) vyhodnotit případné škody, které by utrpěl (správce či třetí osoby), pokud by ke zpracování osobních údajů nedošlo, (iii) zhodnotit povahu zpracovávaných osobních údajů (běžné údaje, zvláštní kategorie údajů), (iv) zvážit své postavení a postavení subjektů údajů (zda jde například o subjekty ve slabším postavení či jde o zaměstnance), (v) zohlednit způsob zpracování osobních údajů (velký rozsah, profilování, zpřístupnění velkému počtu osob apod.), (vi) zohlednit základní práva a svobody subjektů údajů, které moou být dotčeny, (vii) uvážit, zda subjekty údajů mohou zpracování osobních údajů očekávat, a (viii) vyhodnotit dopady na subjekt údajů a porovnat je s očekávanými přínosy zpracování osobních údajů.[361]

V návaznosti na uvedené balancování či posouzení by správce měl dospět k rozhodnutí, zda je zamýšlené zpracování osobních údajů přípustné či nikoliv. Může ovšem také v rámci takového posuzování dospět k závěru, že bude přípustné jen při splnění dalších podmínek. Zejména pokud správce zajistí další odpovídající opatření, jako je minimalizace

[359] Stanovisko WP29 č. 6/2014: K pojmu oprávněných zájmů správce podle článku 7 směrnice 95/46/ES (v originále: *opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC)*. (WP217), ze dne 9. dubna 2014.
[360] Tamtéž, s. 24 až 47.
[361] Tamtéž, s. 56.

zpracovávaných údajů (omezení rozsahu zpracování či krátká doba uchování), odpovídající technická a organizační bezpečnostní opatření (prostřednictvím kterých bude zajištěno, že zpracované údaje nebudou moci být využity pro jiné účely), posouzení vlivu na zpracování osobních údajů, využití technologií posilujících soukromí, zvýšená transparentnost ohledně zpracování (včetně řádného upozornění na právo vznést námitku), zajištění *privacy by design* (jejímž obsahem je povinnost správce údajů jak v době nastavování zpracování, tak i v průběhu zpracování aplikovat technická a organizační opatření k zajištění toho, aby zpracování osobních údajů probíhalo v souladu s nařízením GDPR),[362] či dokonce anonymizace údajů (pak by se již nicméně nejednalo o zpracování osobních údajů).[363]

V souladu se zásadou odpovědnosti by měl být správce schopen doložit, že balanční test vykonal, a měl by jasně zachytit a zdokumentovat, že provedl výše zmíněné kroky v rámci posuzování, zda je možné zpracování osobních údajů realizovat. Tato dokumentace pak bude správci samozřejmě sloužit při kontrolách ze strany ÚOOÚ, správce ji však též může v souladu se zmíněnou zvýšenou transparentností zveřejnit. Samozřejmě v určitých pasážích zveřejnění nemusí být vhodné, například pokud by v balančním testu měla být blíže specifikována jednotlivá opatření pro zabezpečení zpracování osobních údajů. Takovou pasáž by proto bylo pro tyto účely nutné odstranit.

Se zpracováním osobních údajů s odkazem na oprávněný zájem je ruku v ruce spojeno právo subjektu údajů vznést námitku proti zpracování ve smyslu čl. 21 GDPR. Možnost vznesení námitky, která by byla vždy úspěšná, může být samozřejmě též jedním z důvodů pro rozhodnutí správce o zahájení zpracování s odkazem na tento právní základ, neboť v případě vznesení námitky se subjekt údajů ze zpracování vždy automaticky sám efektivně vyloučí. I takové případy mohou být přitom relevantní ve vztahu mezi zaměstnancem a zaměstnavatelem. Zpracováním, které by mohl zaměstnavatel provádět s odkazem na svůj oprávněný zájem, by mohlo být například zpracování fotografií zaměstnanců v rámci intranetu, e-mailového nástroje, interního telefonního seznamu či jiného obdobného nástroje pro sdílení informací u zaměstnavatele, kdy účelem zpracování bude především usnadnění komunikace mezi jednotlivými zaměstnanci. Přitom by platilo, že pokud by se proti tomuto zaměstnanec ohradil, jeho fotografie by jednoduše z daného

---

[362] Nonnemann, F. *Privacy by design jako jedno z nových pravidel pro zpracování osobních údajů?* © EPRAVO.CZ. Publikováno dne 20. dubna 2018. [online]. [cit. 2019-03-02]. Dostupné z: https://www.epravo.cz/top/clanky/privacy-by-design-jako-jedno-z-novych-pravidel-pro-zpracovani-osobnich-udaju-107367.html

[363] Op. cit. sub. 361.

nástroje byla odstraněna. Může jít ale též o případy, kdy zaměstnavatel po určitou dobu zpracovává osobní údaje uchazečů o zaměstnání, aniž by k tomu měl jejich souhlas.[364]

Výše zmíněné konkrétní případy však nebudí příliš pochybností. Sporné budou naopak případy, kdy automaticky úspěšné vznesení námitky umožněno nebude a kdy bude zaměstnavatel vždy prokazovat, že mu svědčí závažné oprávněné důvody pro zpracování ve smyslu čl. 21 odst. 1 GDPR. Půjde zejména o tolik kontroverzní situace, kdy zaměstnavatel provádí nejrůznější kontroly svých zaměstnanců a kdy mu nesvědčí natolik určitá právní povinnost pro provádění kontrol, aby se mohl opírat o právní základ „plnění právní povinnosti" (například kontrola plnění pracovních povinností, kontrola využívání výrobních a pracovních prostředků zaměstnavatele, prevence a detekce podvodného jednání zaměstnanců).

V určitém rozsahu, který bude přesahovat plnění zákonných povinností zaměstnavatelů, se bude jednat též o případy řízení výkonu zaměstnanců a jejich hodnocení.[365] Jiným příkladem může být také, pokud bude zaměstnavatel zpracovávat osobní údaje pro (potenciální či faktické) vymáhání svých pohledávek vůči zaměstnanci. Ani v takovém případě nebude zaměstnanci umožněno úspěšné vznesení námitky, jelikož zaměstnavatel bude údaje potřebovat pro určení, výkon nebo obhajobu právních nároků.[366]

Výše uvedené lze shrnout tak, že zaměstnavateli nepochybně může svědčit celá řada oprávněných zájmů na zpracování osobních údajů, které bude odpovídat stejně široké množství účelů zpracování. S ohledem na skutečnost, že zaměstnanec je ve slabším postavení vůči zaměstnavateli, bude muset zaměstnavatel tuto skutečnost vždy při provádění balančního testu zohlednit a nabídnout dostatečné záruky ochrany základních práv a svobod zaměstnance, aby tuto nerovnováhu vyvážil a mohl zamýšlené zpracování realizovat. Nebudou to přitom jen povinnosti vyplývající z nařízení GDPR, které bude muset zaměstnavatel zohledňovat. Vždy bude muset také uvažovat ochranu zaměstnanců poskytovanou příslušnými ustanoveními ZPr,[367] a proto bude zaměstnavatel při rozhodování o zpracováních osobních údajů na základě oprávněného zájmu vždy velmi omezen.

---

[364] Blíže viz následující bod.

[365] Hranice, kdy se bude ještě jednat o zpracování s odkazem na plnění právní povinnosti a kdy už s odkazem na oprávněný zájem, nemusí být vždy zcela ostrá. Obecně lze nicméně konstatovat, že plnění právní povinnosti by mělo být využitelné jen v těch případech, kdy bude příslušná právní povinnost natolik určitá, aby nepřipouštěla pochybnosti o tom, zda je zamýšlené zpracování osobních údajů nutné plnit či nikoliv.

[366] Srov. čl. 21 odst. 1, věta druhá GDPR.

[367] Zejména ochrana zakotvená v rámci ustanovení § 316 Zpr.

6.2.4 Souhlas

Posledním z právních základů, které mají značný význam z hlediska zpracování osobních údajů zaměstnanců, je zpracování založené na souhlasu dotčeného subjektu údajů, tedy zaměstnance. Souhlasem se dle čl. 4 bodu 11) GDPR rozumí *„jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“*. Každý z těchto přívlastků (svobodný, konkrétní, informovaný a jednoznačný projev vůle) má přitom důležitý význam pro platnost souhlasu. Zejména tedy nesmí být souhlas žádným způsobem vynucován,[368] musí být souhlas spojen s určitým účelem zpracování osobních údajů, subjektu údajů musí být poskytnuty veškeré informace ve smyslu čl. 13 či čl. 14 GDPR, nesmí být ani pochyb o tom, že při určitém jednáním je souhlas udělován či nikoliv.

Pokud jde o způsob udělení, z uvedené definice je zřejmé, že na souhlas nejsou kladeny žádné formální požadavky a platný může být souhlas ústní (u ústního by nicméně mohly být problémy s doložitelností, jak bude vysvětleno dále) i písemný, může být též udělen elektronicky, zejména zaškrtnutím či potvrzením určitého pole na počítači či v mobilním telefonu, může být projeven též odesláním potvrzení v listinné (dopis), elektronické (e-mail) či jiné formě. Naopak za platné udělení souhlasu podle názoru autora této práce nelze považovat konkludentní udělení souhlasu, neboť lze vést závažné pochybnosti o tom, že by se jednalo o jednoznačný projev vůle, a navíc by takový projev nebyl obvykle doložitelný a špatně by se dokládaly i jiné požadavky na platný souhlas, jako je informovanost.[369] To platí obzvláště na pracovišti ve vztahu mezi zaměstnancem a zaměstnavatelem.

Bližší podmínky pro vyjádření souhlasu jsou také dále upraveny v čl. 7 nařízení GDPR. Jak už bylo naznačeno, souhlas musí být správcem doložitelný, a proto je v podstatě vyloučeno udělení souhlasu mlčky a omezeno udělování souhlasu ústně.[370] V případě písemného souhlasu, kdy se písemné prohlášení týká též jiných skutečností, musí být souhlas

---

[368] Toto plně koresponduje s ustanovením § 587 ObčZ, které dává možnost dovolávat se neplatnosti právních jednání pro případ, že k takovému jednání bude osoba přinucena.

[369] Odlišně Nulíček in Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 148.

[370] Ústní udělení souhlasu je možné v situacích, kde bude možné z okolností dovodit, že souhlas by udělen, např. protože subjekt údajů poskytl údaje, který by správce jinak neměl. Omezeně lze uvažovat o platném udělení souhlasu mlčky, například v případě fotografování osoby, která se dobrovolně a vědomě postaví do hledáčku fotoaparátu při skupinovém focení (srov. stanovisko WP29 č. 15/2011: K definici souhlasu (v originále: *on the definition of consent*). (WP187), ze dne 13. července 2011, s. 22).

jasně oddělitelný od těchto jiných skutečností.[371] Tato skutečnost míří na v praxi tradiční vkládání souhlasů do smluv či všeobecných obchodních podmínek, kdy subjekt v podstatě nemá jinou možnost než smlouvu podepsat a souhlas se zpracováním osobních údajů udělit. Takový souhlas by byl tedy nepochybně neplatný.[372] S tím úzce souvisí i podmínka vyjádřená v čl. 7 odst. 4 GDPR, podle které správce nesmí podmiňovat uzavření smlouvy udělením souhlasu.[373]

Pojmovým znakem souhlasu jakožto jednostranného občanskoprávního jednání, je samozřejmě také možnost jej odvolat, jak platí dle čl. 7 odst. 3 GDPR. V té souvislosti je třeba poznamenat, že správce musí na existenci práva odvolat souhlas vždy upozornit a subjektu údajů nemohou být kladeny větší překážky pro odvolání souhlasu, než jaké jsou stanoveny pro jeho udělení. Zakázány tak mají být zejména praktiky, kdy lze souhlas bez dalšího udělit na webu a pro odvolání je nutné zaslat písemnou žádost s úředně ověřeným podpisem na určitou konkrétní adresu. Odvolání souhlasu nebude mít vliv na legálnost či nelegálnost zpracování osobních údajů v době, kdy byl souhlas udělen. Je zřejmé, že po jeho odvolání již osobní údaje nemohou být zpracovávány na tomto právním základě, v omezeném rozsahu však může mít správce jiný právní základ (zejména oprávněný zájem) pro zpracování osobních údajů.

Z výše uvedeného je nepochybné, že získání souhlasu ze strany subjektu údajů by mělo být při zpracování osobních údajů obvykle využíváno v nejmenší míře s ohledem na nestálost tohoto právního základu vzhledem k jeho odvolatelnosti. Z hlediska historického kontextu lze vést určité polemiky o tom, do jaké míry byl souhlas se zpracováním osobních údajů podle ZOOÚ pojmově a definičně srovnatelný se souhlasem dle nařízení GDPR. Podle názoru autora této práce s přijetím nařízení GDPR v podstatě k žádnému praktickému posunu nedošlo.[374] Formulace využívaná ZOOÚ, kdy byl souhlas preferovaným právním

[371] Srov. čl. 7 odst. 2 GDPR.
[372] Snad jen pro úplnost lze poznamenat, že toto nevylučuje, aby souhlas byl do smlouvy či všeobecných obchodních podmínek skutečně vložen. V takové situaci bude pouze nutné dát subjektu údajů najevo (například prostřednictvím samostatného zvýrazněného pole), že je tázán na udělení souhlasu, a vyžádat si samostatné udělení souhlasu, nezávisle na podpisu smlouvy jako takové.
[373] Srov. blíže preambule (43) nařízení GDPR. Toto může být relativně problematické u akceptace různých zákaznických či marketingových soutěží. Řešení však podle názoru autora této práce spočívá v možnosti určení jiného právního základu pro zpracování osobních údajů (zejména plnění smlouvy a oprávněný zájem správce spolu s *opt-out* možností vznesení námitky proti zpracování).
[374] Odlišně Nulíček in Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 125.

základem pro zpracování osobních údajů, byla překonaná stanovisky ÚOOÚ[375] a odporovala i stanoviskům WP29.[376]

Pokud jde o nově explicitně vymezené podmínky pro souhlas vymezené v čl. 7 GDPR, i ty byly již dříve dovozovány. Kdo například před účinností nařízení GDPR zahrnoval souhlas do všeobecných obchodních podmínek, minimálně si musel být jist, že tento způsob bude konfrontován s názory ÚOOÚ.[377]

Bohužel těmto výkladovým nejasnostem nepřidávala ani značná část právnické veřejnosti, kdy souhlas byl tradičně využíván jako právní základ využívaný v podstatě na veškeré činnosti zpracování (zejména v rámci smluv bylo běžné identifikovat požadavek na souhlas, ačkoliv jeho požadování bylo nadbytečně, jelikož údaje byly nezbytné pro splnění smlouvy). S lítostí lze pak konstatovat, že ani výrazná osvěta pravidel zpracování osobních údajů, kterou přineslo nařízení GDPR, tomuto problému příliš nepomohla.[378] Bez ohledu na tyto trvající praktické obtíže nejsou dnes v odborné veřejnosti pochyby o postavení souhlasu jako právního základu pro zpracování a o požadavcích na jeho získání.[379]

Tím se otevírají možnosti pro bližší zkoumání jednotlivých životních situací, v rámci kterých je souhlas se zpracováním osobních údajů vyžadován. Jednou z takových situací je též vztah mezi zaměstnancem a zaměstnavatelem. Jde o velmi specifickou oblast s ohledem na zřejmou skutečnost, jíž je silnější postavení zaměstnavatele, které mu umožňuje vyvíjet určitý nátlak na zaměstnance. V případě, že bude zaměstnanec o souhlas požádán, může mít v mnohých případech odůvodněné obavy, že neudělení souhlasu bude mít pro něj nepříznivé dopady. Ty mohou v extrémních případech spočívat i v odepření variabilní složky jeho

---

[375] Již v roce 2014 ve svém stanovisku Úřad pro ochranu osobních údajů dovozoval: „*Ze zákona však jednoznačně plyne, že všechny právní tituly jsou si rovnocenné v tom smyslu, že postačí, pokud správce může konkrétní zpracování opřít o jakýkoliv jeden z nich…*“ (srov. stanovisko ÚOOÚ č. 3/2014: *K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti*. Srpen 2014.). Situaci však nijak nezlepšovala odborná literatura, která i nadále vyzdvihovala souhlas jako právní základ pro zpracování osobních údajů (srov. Bartík, V., Janečková, E. *Zákon o ochraně osobních údajů s komentářem*. Olomouc: ANAG, 2010, s. 86.).

[376] Stanovisko WP29 č. 15/2011: K definici souhlasu (v originále: *on the definition of consent*). (WP187), ze dne 13. července 2011, s. 7.

[377] Srov. stanovisko ÚOOÚ č. 2/2011: *Zpracování osobních údajů na základě souhlasu ve smlouvě nebo Všeobecných obchodních podmínkách a s tím související problémy*. Srpen 2011, aktualizace únor 2014.

[378] Srov. ÚOOÚ: Tisková zpráva. *Sdělení předsedkyně Úřadu k vyžadování souhlasu*. Publikováno dne 31. srpna 2018 [online]. [cit. 2019-03-08]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31695 a ÚOOÚ: Tisková zpráva. *Poznatky Úřadu k používání GDPR*. Publikováno dne 9. listopadu 2018 [online]. [cit. 2019-03-08]. Dostupné z: https://www.uoou.cz/poznatky-uradu-k-nbsp-pouzivani-gdpr/d-32252

[379] Praktický přehled využít souhlasu v praxi formou otázek a odpovědí nabízí ÚOOÚ na svých webových stránkách, viz ÚOOÚ: Sekce: často kladené dotazy. *K vyžadování souhlasu* [online]. [cit. 2019-03-11]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5047&n=k-vyzadovani-souhlasu

odměny, odepření využívání pracovních benefitů, jako je služební auto či notebook, nebo dokonce v zabránění kariérního postupu.

Z výše uvedených důvodů je této otázce věnována značná pozornost. Již v roce 2001 dospěla WP29 k závěru, že spoléhání se na souhlas ze strany zaměstnavatelů je možné jen v případech, kdy má zaměstnanec skutečně svobodnou volbu a je mu umožněno jej bez újmy odvolat.[380] Následně v roce 2017 dokonce WP29 uzavřela, že *„zaměstnanci nejsou téměř nikdy v postavení, aby mohli dát souhlas svobodně nebo ho odmítnout či odvolat, což je dáno závislostí vyplývající ze vztahu zaměstnavatel/zaměstnanec. Vzhledem k nerovnováze sil mohou zaměstnanci udělit svobodný souhlas jen za výjimečných okolností, kdy souhlas nebo odmítnutí nevyvolá žádné následky".*[381] Podobné závěry lze dohledat též v odborné literatuře[382] a ztotožňuje se s nimi i autor této práce. Poté, co došlo k nahrazení ZOOÚ nařízením GDPR a utichly jakékoliv pochybnosti o tom, že by souhlas měl být preferovaným právním titulem, nic nebrání tomu, aby se tyto závěry projevily též plně v praxi, a nelze si než přát, že do budoucna dojde k odstranění souhlasů ze vzorů pracovních smluv, což bylo dříve velmi časté, a využívání souhlasů na pracovišti bude omezeno jen na vybrané specifické případy.

Z praktického hlediska tedy ještě zbývá odpovědět na otázku, v jakých výjimečných či specifických případech je souhlas jako právní základ pro zpracování osobních údajů akceptovatelný. Nonnemann v této souvislosti zmiňuje, že by se mělo jednat o *„doplňkové zpracování osobních údajů, které pro řádný výkon práce a práv a povinností zaměstnavatele není nezbytné".*[383] S tím se lze nepochybně ztotožnit. Nepochybně musí jít o případy, kdy bude zaměstnanci bez jakékoliv újmy umožněno souhlas odvolat. Mohlo by se jednat například o situace týkající se umístění fotografií či jiných identifikačních údajů zaměstnanců pro potřeby identifikace v rámci interního seznamu nebo na kartičce zaměstnance (pokud by pro tyto účely nebyl zvolen jako základ oprávněný zájem).[384] Dalším relevantním příkladem by mohlo být získávání souhlasu s pořízením a dalším využitím fotografií na firemní akci.

---

[380] Stanovisko WP29 č. 8/2001: Zpracování osobních údajů v kontextu zaměstnání (v originále: *on the processing of personal data in the employment context*). (WP48), ze dne 13. září 2001, s. 23.
[381] stanovisko WP29 č. 2/2017: Zpracování údajů na pracovišti (v originále: *opinion 2/2017 on data processing at work*). (WP249), ze dne 8. června 2017, s. 19.
[382] Srov. například Nonemann, F. *Soukromí na pracovišti*. Právní rozhledy. 2015, 23 (7), s. 235, nebo Morávek, J. Ochrana osobních údajů v pracovněprávních vztazích. Praha: Wolters Kluwer ČR, 2013, s. 407.
[383] Nonemann, F. *Soukromí na pracovišti*. Právní rozhledy. 2015, 23 (7), s. 235.
[384] Srov. výklad v bodě 6.2.3.

(a) Nábor zaměstnanců

Nepochybně bude také namístě získávání souhlasu od uchazečů o zaměstnání (pro potřeby zařazení uchazeče do databáze), zde je však v podstatě mizivý problém vztahu mezi zaměstnancem a zaměstnavatelem spočívající v silnějším postavení zaměstnavatele. V této situaci je navíc nutné důsledně odlišovat fázi, kdy probíhá výběrové řízení na určitou pozici a kdy zaměstnavatel souhlas uchazeče ke zpracování jeho osobních údajů nepotřebuje (v takovém případě je zpracování nezbytné pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů ve smyslu čl. 6 odst. 1 písm. b) GDPR), a fázi, kdy má být uchazeč o zaměstnání na určitou delší dobu zařazen do databáze uchazečů.[385]

K této otázce se již dříve vyjádřil ÚOOÚ, který ve svém rozhodnutí ze dne 29. 5. 2008, č. j. SKO-0629/07, dospěl k závěru že *„v předmětné věci mohl účastník řízení bez souhlasu uchazeče zpracovávat jeho osobní údaje pouze do okamžiku, kdy mu sdělil, že nebyl na pracovní místo vybrán. Pro další zpracování jeho osobních údajů by poté musel mít jeho prokazatelný souhlas, neboť nepřijatý uchazeč oprávněně předpokládal, že jednání o uzavření pracovní smlouvy bylo ukončeno.“*.[386] Podle názoru autora této práce je však toto rozhodnutí, byť částečně, překonáno. Nařízení GDPR totiž na rozdíl od ZOOÚ již tolik nelpí na souhlasu jakožto právním základu pro zpracování osobních údajů, a tak by bezprostředně po ukončení výběrového řízení mohl mít zaměstnavatel též po omezenou dobu (například 2 měsíce) oprávněný zájem si osobní údaje zaměstnance ponechat. Tímto by přitom nijak výrazněji nezasahoval do práv a svobod zaměstnance ve smyslu čl. 6 odst. 1 písm. f) GDPR, neboť osobní údaje zaměstnance již měl a pouze si je ještě krátce ponechá, což může být ve výsledku výhodné i pro uchazeče. Může nastat například situace, že původně vybraný zaměstnanec se po krátké době ukáže být na danou pozici nevhodným, a v takovém případě by zaměstnavatel mohl uzavřít pracovní poměr s jiným vhodným (původně však nevybraným) uchazečem, aniž by byl nucen výběrové řízení opakovat. Samozřejmě musí jít opravdu o omezenou dobu a pro dlouhodobé zpracování osobních údajů uchazeče bude nutné již využít souhlas se zpracováním osobních údajů.

---

[385] Souhlas se zpracováním osobních údajů při zařazování do databáze je dokonce vyžadován zákonem v případě zpracování osobních údajů ze strany krajských poboček úřadu práce či agentur práce (srov. § 17 odst. 2 ZoZ).

[386] Rozhodnutí ÚOOÚ ze dne 29. 5. 2008, č.j. SKO-0629/07. Rozhodnutí ÚOOÚ bylo následně potvrzeno též v rozhodnutí Městského soudu v Praze ze dne 16. 10. 2012, sp.zn. 6 Ca 378/2008.

(b) Skončení pracovního vztahu

Pokud jde o fázi skončení pracovního poměru, situace se od náboru uchazečů liší. Vůči bývalým zaměstnancům totiž v určitých (nikoliv výjimečných) případech může zaměstnavatel nadále přímo či nepřímo vyvíjet určitý nátlak (prostřednictvím pracovního posudku, navýšení odstupného apod.). Na druhou stranu zaměstnavatel v této fázi již obvykle nebude mít zájem na dalším či novém zpracování osobních údajů, které doposud neměl. To ale nebude platit vždy. I v této fázi mohou nastat situace, kdy by zaměstnavatel chtěl zpracovávat nový rozsah údajů a kde by bylo obvykle nutné dovozovat neplatnost souhlasu. Může jít například o situaci, kdy by zaměstnavatel chtěl od bývalého zaměstnance souhlas s přístupem do jeho (bývalé) zaměstnanecké e-mailové schránky. Naopak v zásadě bezkonfliktní situace bude, pokud by souhlas měl být získáván proto, aby osobní údaje bývalého zaměstnance byly zpracovávány v souvislosti s vedením databáze bývalých zaměstnanců, kdy účelem bude pořádání setkání bývalých zaměstnanců či poskytování jiných benefitů.

(c) Trvání pracovněprávního vztahu

Za naprosto nevhodné bude naopak nutné považovat, pokud by zaměstnavatel vyžadoval souhlas s využitím jakýchkoliv kontrolních mechanismů vůči zaměstnanci. To platí bez ohledu na zvolené prostředky (GPS, kamery, systémové sledování využívání informačních technologií) a způsoby kontrol (skryté či otevřené sledování, soustavné, či dokonce jednorázové sledování). V takových případech lze obecně uzavřít, že takový souhlas bude vždy neplatný. Vedle toho budou také případy, kdy vyžadování souhlasu může být sporné a bude záviset na posouzení konkrétních skutkových okolností, zda jeho vyžadování bylo platné, či nikoliv. Například pokud zaměstnavatel vyžaduje souhlas zaměstnance se zveřejněním fotografie na webu a všichni ostatní zaměstnanci fotografii na webu uveřejněnou mají, zaměstnanec je nepochybně vystaven určitému tlaku, který bude zpochybňovat platnost souhlasu. Pokud ale polovina zaměstnanců fotografii na webu zveřejněnou mít bude a polovina nikoliv, pak by bylo spíše možné uzavřít, že se jedná o platné vyžadování souhlasu.

6.2.5 Více právních základů

Jak bylo naznačeno v rámci výkladu o právním základu zpracování osobních údajů s odkazem na plnění právní povinnosti, mohou a budou se dva či více právních základů v určité míře překrývat. V případě zaměstnanců budou osobní údaje v podstatě vždy

zpracovávány pro více než jeden účel. V některých případech mohou spolu takovéto účely souviset, například již zmíněné zpracování osobních údajů pro účely výplaty odměny zaměstnanců a pro splnění zákonných povinností. V jiných případech mohou být tyto účely relativně nezávislé, například pokud jsou údaje o zdravotní způsobilosti a případných zdravotních omezeních zpracovávány pro plnění zákonné povinnosti a pro potřeby řízení lidských zdrojů a souvisejícího posuzování možnosti změn pracovních pozic jednotlivých zaměstnanců.

Uvedené samozřejmě vyvolává otázku, do jaké míry musí zaměstnavatelé jednotlivé (rozdílné) účely specifikovat a poskytovat odpovídající informace v rámci plnění informační povinnosti. Jak již bylo nastíněno při výkladu o účelech,[387] je nutné hledat takovou míru detailu, která je dostatečně určitá a omezuje možnost vznesení pochybností o skutečném účelu zpracování. Při tom je vhodné využít konceptu zastřešujících účelů a nabídnout subjektům údajů možnost získání bližších informací k účelům, pokud je prvotní informace relativně obecnější.[388] V každém případě nicméně platí, že pokud jsou údaje zpracovávány pro více účelů, požadavky stanovené nařízením GDPR se aplikují shodně na každý účel zpracování. To například znamená, že v každém případě bude nutné posuzovat zásadu minimalizace a údaje, které budou pro některý účel zpracování nezbytné, obvykle nemusí být nezbytné pro jiný účel zpracování.

Otázka zpracování osobních údajů pro více účelů (a s odkazem na více právních základů) též úzce souvisí s posouzením možnosti dalšího zpracování ve smyslu čl. 6 odst. 4 nařízení GDPR. Pokud správce zamýšlí provádět takové další zpracování a nezamýšlí v té souvislosti získávat souhlas subjektů údajů ani mu takové zpracování neukládá zákon, musí provést tzv. test slučitelnosti, v rámci kterého musí posoudit zákonnost takového zpracování. GDPR přitom demonstrativně vymezuje pět hledisek, která musí správce při takovém testu zohlednit.[389] I když půjde spíše o méně časté a méně závažné případy, může se zaměstnavatel dostat do pozice, kdy bude nucen tento test slučitelnosti provádět i při zpracování osobních

---

[387] Blíže viz úvodní část podkapitoly 6.2.

[388] Stanovisko WP29 č. 3/2013: K účelovému omezení (v originále: *opinion 3/2013 on purpose limitation).* (WP203), ze dne 2. dubna 2013, s. 53.

[389] Podle ustanovení čl. 6 odst. 4 nařízení GDPR platí, že v rámci testu slučitelnosti správce zohlední mimo jiné: *„a) jakoukoli vazbu mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování; b) okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a správcem; c) povahu osobních údajů, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů podle článku 9 nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů podle článku 10; d) možné důsledky zamýšleného dalšího zpracování pro subjekty údajů; e) existenci vhodných záruk, mezi něž může patřit šifrování nebo pseudonymizace“.*

údajů zaměstnanců. K takovým situacím u zaměstnavatele bude obvykle docházet pouze ve vztahu k některým osobním údajům, například zaměstnavatel může poskytnout určitý benefit zaměstnancům, kteří jsou rodiči, a pro tyto účely vyjde z informací, které má pro účely vypracování daňových přiznání zaměstnanců a uplatňování příslušných slev na děti. Takové další zpracování by bylo nepochybně slučitelné. Naopak pokud by zaměstnavatel využíval údaje o zaměstnanci pro potřeby sledování zaměstnance a zjištění různých údajů o jeho soukromém životě, takové další zpracování by bylo jistě nepřípustné.

7 Zásady a vybrané aspekty zpracování údajů zaměstnanců

7.1 Transparentnost

Další ze základních zásad, které stanoví nařízení GDPR, je zásada transparentnosti. Ta nespočívá jen v plnění informační povinnosti, tedy v poskytování všech informací stanovených v čl. 13 a 14 GDPR, ale též v poskytování sdělení podle článků 15 až 22 GDPR, v povinnosti reagovat na ně ve stanovené lhůtě, jak je blíže specifikováno v čl. 12 nařízení GDPR, ale také v obecném přístupu k poskytování srozumitelných informací. WP29 v této souvislosti rozlišuje tři základní oblasti transparentnosti, a to (i) poskytování stanovených informací subjektům údajů, (ii) komunikaci mezi správcem a subjektem údajů a (iii) usnadnění výkonu práv subjektu údajů.[390] Záměrem této podkapitoly nicméně není zkoumat zásadu transparentnosti v obecné rovině, jak vyplývá z nařízení GDPR, ale analyzovat uplatňování této zásady ve vztahu mezi zaměstnancem a zaměstnavatelem.

Plnění informační povinnosti zaměstnavatelem obvykle nebude komplikované. Zaměstnavatel bude obvykle plnit jen informační povinnost ve smyslu čl. 13 GDPR, neboť údaje v naprosté většině získává od zaměstnanců. Pokud jde o způsob, kdy a jak by zaměstnavatel mohl a měl plnit informační povinnosti, nabízí se, aby stanovené informace poskytoval zaměstnancům již při jejich nástupu. Například v rámci informačního balíku, který je povinen zaměstnancům poskytnout při nástupu.[391] Nulíček v této souvislosti uvádí: *„Dalším způsobem pro větší dosažení srozumitelnosti a přehlednosti je informování subjektu až v okamžiku, kdy je to opravdu nezbytné.“*[392] S takovým závěrem se autor této práce neztotožňuje a domnívá se, že požadované informace musí vždy být poskytnuty již na začátku spolu se zahájením zpracování.

Lze nicméně souhlasit s tím, že v souladu se zásadou transparentnosti dále bude, pokud informace o zpracování osobních údajů zaměstnavatel zveřejní také na místě či způsobem, který zaměstnancům umožní kdykoliv se s těmito informacemi seznámit i později. Nabízí se například umístění příslušného informačního dokumentu[393] na nástěnku

---

[390] Srov. WP29: Pokyny k transparentnosti podle nařízení 2016/679. (WP 260 rev. 01), vydané dne 29. listopadu 2017, ve znění ze dne 11. dubna 2018, s. 4.
[391] Srov. § 37 ZPr.
[392] Nulíček in Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 182.
[393] Informační dokument bývá obvykle označován jako informační memorandum, zásady zpracování osobních údajů, nakládání s osobními údaji, poučení o zpracování osobních údajů, informace o zpracování, směrnice o zpracování, nebo anglicky též jako *privacy policy*.

či jiné místo, kam mají zaměstnanci přístup, kopii by měl mít u sebe k nahlédnutí vždy pověřený zaměstnanec. V dnešní době, kdy jsou při plnění pracovních úkolů používány počítače, se nabízí též umístění dokumentu v rámci sdílených disků či informačních systémů, které zaměstnanci využívají. Vhodné je též umístit informační dokument na intranet, má-li jej zaměstnavatel.

Důležité je, aby poskytované informace byly vždy srozumitelné. Toho zaměstnavatel docílí tím, že poskytované informace nebudou příliš složité a budou jednoduché k pochopení. Jako vhodná forma se nabízí například kladení otázek a odpovědí. Zaměstnavatel by přitom měl obsahově informace uzpůsobit tomu, o jakou cílovou skupinu zaměstnanců se jedná (například zda jde o výrobní zaměstnance, zda se jedná o IT specialisty či právníky),[394] a neměl by se nikdy vymlouvat na nemožnost takového uzpůsobení z jeho strany. Vždy má totiž možnost se svých zaměstnanců dotázat a ověřit u nich tuto skutečnost.[395] Vhodným nástrojem je také již zmiňovaná vrstevnatost, která je doporučována WP29, a související poskytování informací ve vrstvách, které si zaměstnanci mohou v případě zájmu blíže rozbalit a získat tak bližší informace.[396] Auto této práce by zejména chtěl negativně hodnotit mnohastránkové dokumenty, které poskytují přemíru informací, v mnoha částech pouze opisují nařízení GDPR a jsou složité i pro samotné právníky. Takové dokumenty by určitě neměly být považovány za správný přístup k této otázce.

Pokud jde o uplatňování práv ze strany zaměstnanců, měl by být vždy určen konkrétní zaměstnanec, který bude takové žádosti přijímat a vyřizovat. S ohledem na charakter osobních údajů zaměstnanců by se vždy mělo jednat o zaměstnance personálního oddělení, resp. zaměstnance majícího na starosti zaměstnanecké otázky, u kterého bude vždy zajištěno dodržování odpovídající mlčenlivosti. Nařízení GDPR přitom jasně určuje, jaké lhůty a postup by při takovém vyřizování měly být dodržovány (srov. čl. 12 odst. 3 až 5 GDPR). Zaměstnavatel by zároveň nikdy neměl narážet na problémy s identifikováním svých zaměstnanců, a proto by obvykle neměl zaměstnance žádat o poskytnutí dodatečných informací k potvrzení totožnosti ve smyslu čl. 12 odst. 6 GDPR. Zejména může očekávat, že e-mail odeslaný ze zaměstnaneckého e-mailu byl napsán skutečně zaměstnancem,

[394] Není vyloučena ani možnost, aby měl zaměstnavatel pro různé kategorie zaměstnanců různé informační dokumenty. To může být vhodné i z jeho pohledu, neboť u těchto odlišných kategorií může docházet k odlišným způsobům zpracování, a to dokonce i z hlediska účelů zpracování.
[395] WP29: Pokyny k transparentnosti podle nařízení 2016/679. (WP 260 rev. 01), vydané dne 29. listopadu 2017, ve znění ze dne 11. dubna 2018, s. 7.
[396] Tamtéž.

kterému byla schránka přidělena. Obdobně při využití svěřeného telefonu a telefonního čísla zaměstnancem. Mohla by sice nastat situace, že zaměstnanci někdo odcizí přístup k e-mailu nebo telefon, ale to by se při dodržování obvyklých povinností ze strany zaměstnance nemělo stát a zaměstnavatel má také určitou možnost takové podvodné jednání rozpoznat (např. podle hlasu, stylu písma apod.). Ostatně ani při ověřování totožnosti jiných subjektů údajů (například zákazníků) nebude obvyklé, aby totožnost jednajících osob byla určena se stoprocentní jistotou.

Při výkladu o zpracování osobních údajů zaměstnanců a plnění informační povinnosti je též vhodné poukázat na skutečnost, že ZPr též v obecné rovině prosazuje transparentnost. V praxi pak dochází k tomu, že se tyto dvě zásady v určitých situacích prolínají či překrývají. Jde zejména o povinnost zaměstnavatele informovat své zaměstnance o prováděných kontrolách ve smyslu § 316 odst. 3 ZPr. V takových případech totiž vždy bude nutně docházet ke zpracování osobních údajů zaměstnanců a zaměstnavatel se nevyhne též povinnosti plnit informační povinnost dle nařízení GDPR. Zaměstnavatel by měl nicméně informovat zaměstnance také o tom, jak bude přiměřeným způsobem kontrolovat, že zaměstnanci nevyužívají svěřené výrobní a pracovní prostředky pro osobní potřebu ve smyslu § 316 odst. 1 ZPr.

Dalším specifikem ZPr, v rámci kterého se střetává transparentnost dle ZPr a nařízení GDPR, je vedení osobního spisu zaměstnance. Jak již bylo zmiňováno, v podstatě veškeré informace vedené v osobním spisu jsou osobními údaji zaměstnance, a i kdyby zaměstnanec neměl k osobnímu spisu přístup ve smyslu § 312 odst. 3 ZPr, mohl by se zaměstnanec domáhat přístupu, resp. poskytnutí kopií s odkazem na čl. 15 GDPR. Právě ale explicitní zmínka o možnosti přístupu v ZPr má důležitý význam (srov. výklad v další podkapitole).

7.2 Práva zaměstnanců

Práva subjektů údajů v souvislosti se zpracováním osobních údajů jsou ve smyslu sktruktury nařízení GDPR obsažená v čl. 12 až 23, a zahrnují tak již výše zmíněná obecná pravidla týkající se transparentnosti a obecnou infomační povinnost. Záměrem této podkapitoly je nicméně věnovat se již analýze specifických práv obsažených v čl. 15 až 22 GDPR. Nad rámec této práce je přitom obecný výklad a analýza těchto jednotlivých práv a jejich interpretačních a jiných problémů. Snahou této podkapitoly proto je věnovat se těm, které mají dopad na vztah mezi zaměstnancem a zaměstnavatelem.

Na úvod této podkapitoly je ještě třeba poznamenat, že úvahy o jednotlivých právech jsou podávány především z toho hlediska, na kolik je jejich uplatňování relevantní ve vztahu mezi zaměstnancem a zaměstnavatelem a dále též nakolik jsou zaměstnanci skutečně svobodní při jejich uplatňování. Na rozdíl od otázky možnosti dobrovolného (a tím i přípustného) udělování souhlasů ze strany zaměstnanců, které je věnována relativně větší pozornost,[397] není tato otázka v takové míře v odborné veřejnosti diskutována, nicméně nelze opomíjet základní skutečnost, že zaměstnanci jsou ve slabším postavení vůči zaměstnavatelům a uplatnění některého z práv zaměstnancem může (nikoliv musí) být zaměstnavatelem vnímáno negativně v tom smyslu, že daného zaměstnance bude nadále v rámci pracovněprávního vztahu znevýhodňovat. Přes osvětu a rozšíření obecného povědomí o ochraně osobních údajů a o možnosti uplatňovat jednotlivá práva, které přineslo nařízení GDPR, je takové uplatňování práv vnímáno správci nadále spíše negativně, a to zejména s ohledem na tu skutečnost, že uplatňování těchto práv není ze strany subjektů údajů příliš časté. Sice se dá konstatovat, že k určitému nárůstu při uplatňování práv došlo, ten však nebyl příliš významný a je otázkou, zda postupem času se počet žádostí nevrátí na stejné hodnoty.[398]

7.2.1 Právo na přístup k osobním údajům

Základním právem, které subjekty údajů mají, je právo na přístup ke zpracovávaným osobním údajům. Na rozdíl od předchozí právní úpravy obsažené v § 12 ZOOÚ, které umožňovalo poskytovat jen kategorie zpracovávaných osobních údajů,[399] není dnes již pochyb o tom, že při uplatnění tohoto práva je nutno poskytovat též kopii zpracovávaných osobních údajů.[400] Takto formulované ustanovení s sebou přináší značné praktické obtíže vyplývající z toho, jak široce je pojem osobního údaje definován. Vyjdeme-li například ze skutečnosti, že zaměstnanci (či kdokoliv jiný) zanechávají

[397] Srov. výklad v části 6.2.4.
[398] V rámci dotazníkového průzkumu mezi účastníky seminářů konaných ÚOOÚ pro pověřence pro ochranu osobních údajů v říjnu 2018 uvedlo 43 ze 75 respondentů (57 %), že využívání práv subjektů údajů je stejné jako dříve, 22 respondentů (30 %) uvedlo, že došlo k mírnému nárůstu a pouze 9 respondentů (7 %) uvedlo, že došlo k výraznému nárůstu (1 respondent neodpověděl); srov. ÚOOÚ: Výsledky dotazníkového průzkumu mezi účastníky seminářů pro pověřence pro ochranu osobních údajů v říjnu 2018. Publikovaná dne 31. října 2018, tabulka č. 5, s. 4. [online]. [cit. 2019-03-20]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32270
[399] Ačkoliv již dříve někteří autoři dovozovali nutnost poskytovat též jednotlivé konkrétní údaje, které jsou zpracovávány, srov. blíže Pospíšil in Kučerová, A. *Zákon o ochraně osobních údajů: komentář.* Praha: C. H. Beck, 2012, s. 224.
[400] Srov. čl. 15 odst. 3 GDPR.

v systémech elektronickou stopu (log) o činnostech, které v těchto systémech prováděli, pak i takováto stopa může být osobním údajem a zaměstnavatel by měl, pokud zaměstnanec uplatní právo na přístup, veškeré tyto informace zaměstnanci poskytnout. Rozsah poskytovaných informací poté může být v podstatě neomezený.

Podle názoru autora této práce je nutné k této otázce přistupovat pragmaticky a hledat skutečný smysl a účel tohoto práva na přístup k osobním údajům. Tím je poskytnout srozumitelné informace o povaze zpracování a nabídnout zaměstnanci možnost udělat si jasnou představu o účelech a rozsahu takového zpracování. Není tudíž nezbytné, aby zaměstnavatel poskytoval veškeré údaje, ale jen ty, které jsou podstatné, a v ostatním může požádat subjekt o bližší specifikaci údajů, které požaduje.[401] Kromě toho by rozsah poskytovaných informací měl být limitován dvěma korektivy, kterými jsou (i) informační hodnota poskytovaných informací v tom smyslu, že pokud by informace neměly žádnou informační hodnotu (např. změť čísel), nemá význam je poskytovat, a (ii) neúměrné obtíže pro správce při získávání takových informací (zvlášť s ohledem na skutečnost, že subjekt údajů může své právo uplatnit bezplatně).[402] Samozřejmostí je také uplatnění třetího korektivu, který je vyjádřen přímo v čl. 15 odst. 4 GDPR, a to, že poskytnutím kopie nesmějí být nepříznivě dotčena práva a svobody jiných osob. To tedy bude do značné míry omezovat možnost poskytování takových osobních údajů, které budou neoddělitelně spojeny s osobními údaji jiné osoby, s obchodním tajemstvím, nebo pokud se bude jednat o duševní vlastnictví.[403]

Dalším problémem, který v souvislosti s právem na přístup k osobním údajům vzniká, je skutečnost, že zaměstnanci mnohdy v praxi neváhají tohoto svého práva využít (či jej zneužít), aby na své zaměstnavatele vytvářeli určitý tlak. Mnohdy k tomu dochází v situacích, kdy zaměstnanec vede se svým zaměstnavatelem určitý spor (který je navíc z hlediska ochrany osobních údajů zaměstnance irelevantní, neboť jde například o ukončení pracovního poměru). Podle názoru autora této práce by zaměstnavatelé měli v takových případech k uplatnění takového práva přistupovat bez ohledu na to, že s dotčeným zaměstnancem je veden spor. Zejména by mu měly být poskytnuty požadované údaje. Pokud

---

[401] S tímto ostatně počítá i nařízení GDPR, které v preambuli (63) uvádí: „*Pokud správce zpracovává velké množství informací týkajících se subjektu údajů, měl by mít možnost před poskytnutím informací požádat subjekt údajů, aby konkrétně uvedl, kterých informací nebo činností zpracování se jeho žádost týká.*“

[402] A to na základě čl. 12 odst. 5 GDPR.

[403] Srov. WP29: *Pokyny týkající se práva na přenositelnost údajů*. (WP242 rev. 01), vydané dne 13. prosince 2016, ve znění ze dne 5. dubna 2017, s. 13, výklad k čl. 20 odst. 4 nařízení GDPR (který je shodný s čl. 15 odst. 4 GDPR).

má zaměstnavatel údajů mnoho, měl by zaměstnance požádat o upřesnění požadovaných údajů. A pokud by snad měly být vyžadovány informace, které jsou z různých důvodů (zejména s ohledem na probíhající spor) citlivé, zaměstnavatel by měl být oprávněn takové údaje odmítnout s odkazem na již zmiňovaný čl. 15 odst. 4 GDPR, neboť by tím mohla být dotčena jeho práva.

Pokud jde o výše nastíněný problém, že uplatnění jednotlivých práv zaměstnancem může v rámci pracovněprávního vztahu vyvolat určitou konfrontaci se zaměstnavatelem (myšleno v situaci, kdy ještě mezi nimi žádný spor nevznikl), je do jisté míry ošetřen samotnými ustanoveními ZPr, a to konkrétně ustanoveními o vedení osobního spisu (§ 312 ZPr). Lze totiž očekávat, že značná část osobních údajů zaměstnance bude v osobním spise obsažena, a jelikož je zaměstnanec oprávněn do svého osobního spisu nahlížet a činit si z něho výpisky či pořizovat stejnopisy v něm obsažených dokladů,[404] bude se moci vyhnout odvolávání se na své právo na přístup podle GDPR, jehož uplatnění by mohlo vzbuzovat negativní emoce. Samozřejmým nedostatkem tohoto postupu je, že osobní spis nebude obsahovat všechny osobní údaje (jen písemnosti nezbytné pro výkon práce). Zejména tedy tímto postupem nemusí získat osobní údaje shromážděné v rámci kontrol prováděných zaměstnavatelem. U takových a dalších osobních údajů nezbyde zaměstnanci než využít svého práva na přístup dle nařízení GDPR.

7.2.2 Právo na výmaz

Další z práv, kterému je vhodné věnovat větší pozornost, je právo na výmaz, resp. právo být zapomenut ve smyslu čl. 17 nařízení GDPR. Co je obsahem tohoto práva, je zřejmé. Jde o právo požadovat u správce, aby došlo k výmazu osobních údajů. Samozřejmě platí, že toto právo nelze uplatit vždy, ale jen za stanovených podmínek (nepotřebnost údajů, odvolání souhlasu, vznesení námitky, protiprávní zpracování apod.) a že v určitých případech se toto právo vůbec neuplatní (zpracování bude nezbytné pro výkon práva na svobodu projevu, splnění právní povinnosti, z důvodů veřejného zájmu apod.).[405] S ohledem na uvedené limity a praktické obtíže při vymáhání tohoto práva se jako přiléhavější jeví Bartošovo označení jako právo na rozmazané vzpomínky.[406]

---

[404] Srov. ustanovení § 312 odst. 3 ZPr.
[405] Srov. čl. 17 GDPR.
[406] BARTOŠ, Vojtěch. *Právo být zapomenut? Spíše právo na rozmazané vzpomínky…* Jiné právo. Publikováno dne 31. května 2014 [online]. [cit. 2019-04-30]. Dostupné z: http://jinepravo.blogspot.com/2014/05/vojtech-bartos-pravo-byt-zapomenut-spis.html

Ač se mnohdy v souvislosti s nařízením GDPR psalo, že právo na výmaz je novinkou, kterou tento právní předpis přináší, je vhodné zmínit, že o úplnou novinku se nejednalo. Již v roce 2014 dovodil SDEU existenci tohoto práva s odkazem na Směrnici, a to v rozhodnutí ve věci C-131/12, Google Spain, ze dne 13. května 2014. V tomto rozhodnutí soud posuzoval oprávněný zájem veřejnosti na zveřejnění určitých informací společností Google proti právu dotčeného subjektu na zveřejňování informací o jeho o sobě. Jak je zřejmé, dal v tomto případě soud za pravdu dotčenému subjektu,[407] což následně vedlo k tomu, že Google na své stránky implementoval formulář, jehož prostřednictvím bylo a je možné o uplatnění tohoto práva žádat.

Pokud jde o uplatnění tohoto práva při zpracování osobních údajů zaměstnanců, lze konstatovat, že bude velmi omezené. S ohledem na analýzu podanou v podkapitole 6.2 této práce je zřejmé, na jakých právních základech budou osobní údaje zaměstnanců nejčastěji zpracovávány. Nejčastěji půjde o zpracování s odkazem na plnění právní povinnosti nebo s odkazem na nezbytnost pro plnění smlouvy. Do úvahy bude připadat též zpracování s odkazem na oprávněný zájem zaměstnavatele. Již velmi okrajovou záležitostí bude zpracování na základě souhlasu zaměstnance.

Poměří-li se tyto závěry s jednotlivými důvody pro možnost požadovat výmaz dle čl. 17 odst. 1 GDPR, budou (u zaměstnavatele zpracovávajícího osobní údaje svých zaměstnanců odpovědně) připadat do úvahy v podstatě jen důvody podle písm. a), tj. osobní údaje již nebudou potřebné pro účely stanovené zaměstnavatelem, a podle písm. c), tj. zaměstnanec vznese námitku proti zpracování. Za doby trvání pracovního poměru by pak mělo být možné tyto důvody uplatnit jen ve vztahu k účelům zpracování, které budou prováděny s odkazem na oprávněný zájem zaměstnavatele. Půjde tedy o rozsahově relativně menší případy zpracování, které jsou v pracovněprávním vztahu spíše doplňkové, o to však více mohou vyvolávat určité kontroverze (jak bylo totiž již zmiňováno, s odkazem na tento právní základ mohou být zpracovávány osobní údaje zaměstnanců například při prováděných kontrolách zaměstnanců).

S výjimkou těchto případů, kdy bude namístě možnost uplatnit námitku a o kterých je blíže pojednáno v další části, lze shrnout, že pokud budou zaměstnavatelé zpracovávat osobní údaje svých zaměstnanců v souladu s právními předpisy a v souladu s pracovní smlouvou, nebude mít právo na výmaz osobních údajů při zpracování osobních údajů

[407] Blíže viz rozhodnutí SDEU ze dne 13. května 2014, C-131/12, ve věci Google Spain.

zaměstnanců většího uplatnění. Po skončení pracovního poměru se situace může do jisté míry změnit. Na druhou stranu platí, že zaměstnavatelé mají i po skončení pracovního poměru celou řadu zákonných povinností, které jim ukládají osobní údaje zpracovávat (blíže viz podkapitola 7.3).

7.2.3 Právo vznést námitku

Jak bylo naznačeno v předchozím bodě 7.2.2, s právem požadovat výmaz úzce souvisí právo vznést námitku proti zpracování ve smyslu čl. 21 GDPR. Tu lze uplatnit především v případě, že je zpracování osobních údajů založeno na oprávněném zájmu správce či třetí osoby.[408] Jak již bylo zmíněno, zpracování osobních údajů zaměstnanců s odkazem na oprávněný zájem bude obvyklé. Pokud zaměstnanci proti takovému zpracování vznesou námitku, bude muset zaměstnavatel prokazovat *„závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů [zaměstnanců], nebo pro určení, výkon nebo obhajobu právních nároků“*.[409] To tedy neznamená, že by zaměstnavatel musel automaticky zpracování ukončit,[410] je však na jeho straně, aby prokázal, že zpracování je skutečně opodstatněné a důvody převáží nad právy a základními svobodami konkrétního zaměstnance. Až pokud by se mu toto prokázat nepodařilo, musel by zpracování ukončit.[411]

Při analýze možnosti uplatnění práva na vznesení námitky stojí též za zmínku skutečnost, že na námitku je nutné upozornit zřetelně a odděleně od jakýchkoliv jiných informací ve smyslu čl. 22 odst. 4 GDPR. Aplikace této povinnosti může při zpracování osobních údajů zaměstnanců vzbuzovat jisté sporné otázky, a to ve spojitosti s povinnostmi zaměstnavatele ve smyslu ZPr. Pokud budeme totiž předpokládat, že při provádění kontrol zaměstnanců ve smyslu ustanovení § 316 odst. 2 ZPr dochází ke zpracování osobních údajů zaměstnanců s odkazem na oprávněný zájem zaměstnavatele a že zaměstnavatel je povinen

---

[408] Vedle toho lze námitku uplatnit též v případě, že zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci a je jím pověřen správce ve smyslu čl. 6 odst. 1 bodu e) GDPR, a v případě, že jsou údaje zpracovávány pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 GDPR. S ohledem na nikoliv obecný charakter těchto možností a nižší míru využitelnosti v pracovněprávních vztazích, nebude těmto možnostem dále věnována pozornost.

[409] Srov. čl. 21 odst. 1 GDPR.

[410] Automaticky ukončit zpracování by bylo nutné pouze v případě zpracování pro účely přímého marketingu dle čl. 21 odst. 2 GDPR.

[411] Odlišně Nulíček, který dovozuje, že osobní údaje je (vždy) nutné přestat zpracovávat, vznese-li subjekt údajů námitku, a pokud chce „následně“ správce zpracovávat jeho osobní údaje, musí prokázat závažné oprávněné důvody pro zpracování (srov. Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 229).

o takovém sledování zaměstnance informovat ve smyslu ustanovení § 316 odst. 3 ZPr, pak by při takovém informování měl v souladu se zásadou transparentnosti upozornit subjekty údajů též na možnost vznesení námitky proti takovému sledování.

Navíc už samotné uplatnění práva vznést námitku proti zpracování, ať už o něm byl zaměstnanec řádně informován, či nikoliv a ať už s tímto právem bude zaměstnanec úspěšný, či nikoliv, nepochybně na pracovišti vzbudí jisté emoce. Na rozdíl od práva na přístup, kde se těchto emocí dalo vyvarovat využitím práva na nahlédnutí do osobního spisu, nenabízí ZPr k tomuto právu žádnou alternativu. Budeme-li uvažovat, že zpracování založené na oprávněném zájmu se týká kontrol zaměstnanců, může nepřímá ochrana proti takovému stavu spočívat v definování podmínek, kdy zaměstnavatel může zaměstnance kontrolovat v rámci § 316 ZPr, a tím pádem ve vyšších nárocích při provádění balančního testu a posuzování převahy zájmů zaměstnavatele nad právy a základními svobodami zaměstnanců. To však nemíří na veškeré případy zpracování s odkazem na oprávněný zájem a ani v případě kontrol prováděných zaměstnavatelem nenabízí stejnou možnost, jako je právo na vznesení námitky. Zaměstnanci proto při pochybnostech o oprávněnosti zpracování jeho osobních údajů nezbude než právo na námitku u zaměstnavatele vznést. De lege ferenda by stálo za úvahu, zda by pro tento případ neměla existovat specifičtější ochrana práv zaměstnanců.

7.2.4 Ostatní práva

Mezi další, dosud nezmíněná práva subjektů údajů patří právo na opravu a doplnění osobních údajů (čl. 16 GDPR), právo na omezení zpracování (čl. 18 GDPR) a právo na přenositelnost osobních údajů (čl. 20 GDPR). Tato práva nebudou v praxi představovat obvykle větší potíže, resp. jejich uplatnění nebude tak časté. Zejména při uplatnění práva na opravu a doplnění u zaměstnavatele by nemělo docházet k větším obtížím. Lze dokonce konstatovat, že je povinností zaměstnavatele mít aktuální a správné osobní údaje svých zaměstnanců.[412]

Pokud jde o právo na omezení zpracování, lze očekávat, že toto bude subjektem údajů uplatňováno jen velmi sporadicky, neboť charakterem se jedná v podstatě o přechodné právo a subjekt údajů bude vždy uplatňovat právo, které takový charakter nemá (např. právo na výmaz, vznesení námitky, popírání přesnosti zpracovávaných údajů apod.). To však nebude

[412] A to zejména s ohledem na povinnosti zaměstnavatele při plnění informačních a oznamovacích povinností vůči orgánům státní zprávy (zejména správa sociálního zabezpečení) či veřejným zdravotním pojišťovnám.

správce za určitých okolností zbavovat povinnosti zpracování omezit. Ustanovení čl. 18 GDPR by totiž dle názoru autora této práce mělo být čteno tak, že správce je povinen zpracování osobních údajů ve stanovených případech omezit vždy sám automaticky (aniž by toto právo bylo subjektem údajů explicitně uplatněno). Jen takovýto závěr je totiž v souladu se zásadami zákonného zpracování a minimalizace údajů (čl. 5 GDPR).

Pokud jde o právo na přenositelnost osobních údajů, za zmínku stojí, že toto právo je jediným právem, které lze označit za novinku, kterou s sebou přineslo nařízení GDPR. Veškerá ostatní práva byla již ve Směrnici, potažmo též v ZOOÚ, obsažena. Při bližší analýze je však patrné, že toto právo je v podstatě jen určitou specifickou podmnožinou práva na přístup k osobním údajům, neboť subjekt údajů by dosáhl podobného (nikoliv shodného) cíle, pokud by uplatnil právo na přístup. WP29 k zavedení tohoto práva uvedla: *„Jednotlivci využívající své právo na přístup k údajům […] byli omezeni formátem zvoleným správcem údajů při poskytování požadovaných informací. Cílem nového práva na přenositelnost údajů je posílení pravomocí subjektů údajů, pokud jde o jejich vlastní osobní údaje, jelikož usnadňuje jejich schopnost své osobní údaje snadno přemísťovat, kopírovat nebo předávat z jednoho informačního prostředí do jiného.“*[413]

Zmiňované usnadnění spočívá zejména v povinnosti poskytovat údaje ve strukturovaném, běžně používaném a strojově čitelném formátu, který subjekt údajů snadno předá jinému správci, resp. který bude jinému správci předán přímo od původního správce. Důležitá je také podmínka, že takové právo lze uplatnit jen k osobním údajům, které jsou zpracovávány pro plnění smlouvy nebo na základě souhlasu subjektu údajů. Autor této práce se domnívá, že přestože značná část osobních údajů zaměstnanců je zpracovávána s odkazem na plnění právní povinnosti, nelze opomíjet, že shodně jsou osobní údaje v určitém rozsahu zpracovávány též pro plnění pracovní smlouvy a na základě toho bude zaměstnanec oprávněn toto právo uplatnit.[414] Svůj význam toto může mít například v situaci, kdy bude zaměstnavatel otálet s vydáním pracovního posudku, nebude chtít pořizovat fyzické kopie určitých dokumentů z osobního spisu[415] nebo pokud bude mít zaměstnanec z jiného důvodu zájem na tom, aby jeho vybrané osobní údaje byly předány zaměstnavateli

[413] Srov. WP29: *Pokyny týkající se práva na přenositelnost údajů.* (WP242 rev. 01), vydané dne 13. prosince 2016, ve znění ze dne 5. dubna 2017, s. 4.
[414] Shodně WP29 (srov. op cit. sub. 413, s. 9.).
[415] U některých tam obsažených dokumentů by však mohlo být sporné, zda jsou v osobním spisu vedeny s odkazem na plnění právní povinnosti či s odkazem na plnění smlouvy. Toto by bylo nutné posuzovat ad hoc dokument od dokumentu.

novému, a to ve strojově čitelném formátu (lze si představit, že zaměstnanec by se s novým zaměstnavatelem mohl dohodnout například na poskytnutí určitých benefitů, pokud prokáže některé informace o své praxi u předchozího zaměstnavatele apod.).

Pro úplnost je nutné dodat, že kromě výše zmíněných práv mají zaměstnanci rovněž právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, které by pro ně mělo právní účinky nebo se jich obdobným způsobem významně dotýkalo (čl. 22 GDPR). I toto právo může být relevantní ve vztahu mezi zaměstnancem a zaměstnavatelem nebo před vznikem tohoto vztahu. Například by u zaměstnavatele mohl existovat automatizovaný systém, který by automaticky vyhodnocoval žádosti uchazečů o zaměstnání a automaticky by je schvaloval či zamítal. Nebo by se mohlo jednat o automatizované monitorovací nástroje, které by dohlížely na pracovní výkonnost zaměstnance, přičemž v případě neplnění by automaticky generovaly výtku vůči zaměstnanci. Z citovaného ustanovení pak jasně vyplývá, že zaměstnanec či uchazeč o zaměstnání má právo na lidský zásah a přezkoumání výsledků takového zpracování a může se tedy bránit před takovýmto automatizovaným rozhodováním.

7.3 Minimalizace údajů

Další z klíčových zásad týkajících se zpracování osobních údajů říká, že osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.[416] Jinými slovy lze vyjádřit tuto zásadu tak, že správce musí při činnostech zpracování využívat jen ty údaje, které nezbytně pro danou činnost potřebuje, a ostatní údaje je naopak povinen nezpracovávat. Jde tedy o minimalizaci zpracovávaných osobních údajů. Z širšího hlediska lze o této zásadě uvažovat jako o obecné povinnosti každého správce posuzovat vždy veškeré varianty zpracování a zvolit jen tu variantu, která do soukromí dotčených subjektů bude zasahovat v nejmenší možné míře.[417]

Takto šířeji vnímaná zásada minimalizace pak spočívá v tom, co nařízení GDPR upravuje ve svém čl. 25 a označuje jako záměrnou a standardní ochranu osobních údajů, resp. pod známějším anglickým spojením jako *privacy by design and by default*. Tento princip či koncept je přitom velmi důležitý z hlediska dodržování zákonného zpracování. Jednoduše jej lze vystihnout tak, že zaměstnavatelé musí před rozhodnutím o variantě

[416] Srov. ustanovení čl. 5 odst. 1 písm. c) GDPR.
[417] Srov. stanovisko ÚOOÚ č. 6/2009: *Ochrana soukromí při zpracování osobních údajů*. Listopad 2009, aktualizace únor 2014.

zpracování osobních údajů volit tu variantu, která je co nejvíce šetrná z hlediska zpracování osobních údajů a zásahů do soukromí. Nonnemann tento koncept shrnuje tak, že jeho *„obsahem je povinnost správce údajů jak v době nastavování parametrů pro nové zpracování osobních údajů, tak i v jeho průběhu, aplikovat technická a organizační opatření k zajištění toho, aby zpracování osobních údajů probíhalo v souladu s obecným nařízením a aby byla ochráněna práva dotčených osob".*[418] Tento popis v zásadě zestručňuje to, co je uvedeno v čl. 25 GDPR, a zdůrazňuje nutnost posuzování této otázky před zahájením zpracování a během něj. Záměrná a standardní ochrana osobních údajů se přitom neváže jen na minimalizaci osobních údajů, ale na posuzování dalších aspektů, zejména zabezpečení zpracování.

Správci musí při plnění této povinnosti přihlížet zejména ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob. Pokud jde o minimalizaci zpracovávaných osobních údajů, je zdůrazněno, že správci musí zavést „*vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti.".*[419] V praxi to bude zejména znamenat, že správci budou muset přizpůsobit své formuláře pro poskytování osobních údajů, spolupracovat s vývojáři aplikací, aby využívané nástroje nezpracovávaly nadbytečné údaje, vybírat hardware, který bude dostatečný pro požadované zpracování,[420] likvidovat nepotřebné dokumenty, zejména listinné dokumenty, nebudou-li potřebné. To vše, aby požadovali a zpracovávali nezbytné minimum údajů.

Při zpracovávání osobních údajů zaměstnanců bude dodržování výše zmíněných principů a pravidel znamenat, že zaměstnavatelé budou muset nastavit své osobní dotazníky a jiné dokumenty tak, aby byly vyžadovány jen nezbytné údaje, zajistit, že jimi využívané systémy budou omezeny na zpracování nezbytných osobních údajů, nebo zajistit, aby přístup k zaměstnaneckým dokumentům a obecně všem údajům byl vyhrazen jen pro určité osoby, které budou vázány odpovídající mlčenlivostí, a aby veškeré osobní údaje zaměstnanců byly

---

[418] Op. cit. sub. 362.
[419] Čl. 25 odst. 2 GDPR.
[420] Například pro monitorování určitých prostor by měla být zvolena jen taková kamera, která dostatečně zajistí sledování určitého prostoru, ale už nezabírá prostor jiný, který monitorován být nemusí.

dostatečně zabezpečeny (ať už jde o fyzické zabezpečení na pracovišti, či technické a jiné zabezpečení v rámci systému zaměstnavatele). Obecně by také mělo být zajištěno, že soubor interních dokumentů či informací, který je potřebný pro fungování zaměstnavatele, bude rovněž minimalizován na nezbytné minimum a dostatečně zajištěn proti zneužití.

Aktuální stav plnění těchto povinností musí zaměstnavatelé průběžně monitorovat a nemohou se spokojit s tím, jaké bylo nastavení na začátku zpracovávání. V průběhu doby se například může ukázat, že zpracování určitých údajů je již nepotřebné. Zejména díky elektronizaci interní komunikace a procesů se vše nejen urychluje, ale je možné vše zachycovat a uchovávat prostřednictvím odpovídajících systémů. Ve velkém proto zaniká potřeba vedení celé řady interních dokumentů, které byly dříve pro fungování společností nezbytné.

Zaměstnavatelé také musí dodržovat to, že určité osobní údaje mohou být využívány jen v situacích, kdy je to nezbytné. V souladu se zásadou účelového omezení totiž platí, že ačkoliv má zaměstnavatel nárok určité údaje zpracovávat, ještě to neznamená, že je může využívat pro veškeré účely. Špatnou praxí je například využívání rodných čísel zaměstnavateli. Ačkoliv má zaměstnavatel nepochybně nárok rodné číslo zpracovávat,[421] není již žádný důvod pro to, aby zaměstnavatel vyžadoval po zaměstnanci uvedení rodného čísla v pracovní smlouvě, nebo dokonce aby zaměstnavatel vedl databázi svých zaměstnanců podle jejich rodných čísel.[422]

7.3.1 Jednotlivé údaje zpracovávané zaměstnavateli

Zaměstnavatelé obvykle získávají osobní údaje o svých zaměstnancích přímo od zaměstnanců v souvislosti se vznikem a trváním pracovněprávního vztahu. Při zahájení pracovního poměru například prostřednictvím osobního dotazníku a dále pouhým plněním práv a povinností vyplývajících ze zákona a z pracovní smlouvy, resp. pracovních povinností ze strany zaměstnance. Za určitých okolností mohou být osobní údaje získávány i z veřejně dostupných zdrojů (to platí zejména před zahájením trvání pracovněprávního vztahu) a mohou být získávány též z vlastní činnosti při hodnocení a zpracování údajů, které zaměstnavatelé od zaměstnanců získávají v souvislosti s trváním pracovněprávního vztahu.

---

[421] Například s odkazem na povinnosti uložené zaměstnavateli zákonem č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů.

[422] Ve vztahu k rodným číslům je toto pravidlo navíc umocněno zvláštní regulací rodných čísel obsaženou v ustanovení § 13c zákona č. 133/2000 Sb., o evidenci obyvatel, ve znění pozdějších předpisů.

Z výše uvedených zdrojů stojí za bližší analýzu zejména údaje získávané zaměstnavateli v souvislosti s nástupem do práce. Platí, že pro jednoznačnou identifikaci osob obvykle stačí znát jeho jméno, bydliště a datum narození. Tato kombinace údajů se obecně považuje za dostatečnou (srov. ustanovení § 3019 ObčZ), nicméně jak bylo zmíněno výše, zaměstnavatel je nepochybně oprávněn či povinen pro určité účely zpracovávat též rodná čísla zaměstnanců. Kromě toho je zaměstnavatel též oprávněn vyžadovat údaje, jako jsou místo narození, pohlaví, místo trvalého pobytu, státní občanství, informace o případném pojištění v zahraničí, o době vojenské činné služby.[423]

Zajímavá je také otázka opisování čísel a kopírování dokladů (zejména občanských průkazů a pasů). Zaměstnavatelé obecně nemají oprávnění takové údaje požadovat. V určitých případech sice jejich pořízení může být odůvodněné (nejčastěji s odkazem na oprávněný zájem určitých zaměstnavatelů vykonávajících specifické činnosti), i tak by si však měli zaměstnavatelé dané údaje pouze opsat a neměli by kopie dokladů pořizovat, a to s ohledem na specifickou regulaci těchto dokladů, která možnost pořizování kopií omezuje (resp. podmiňuje získání souhlasu, nestanoví-li právní předpisy jinak).[424]

Pokud jde o kontaktní údaje zaměstnance, je zaměstnavatel nepochybně oprávněn znát veškeré informace, které mu poskytnul sám zaměstnanec a které budou jejich vzájemnou komunikaci usnadňovat. Kromě adresy trvalého pobytu se může jednat o další adresu (korespondenční), soukromý e-mail, telefonní číslo či číslo mobilního telefonu nebo také o kontakt na sociální síti. V dnešní době je samozřejmostí rovněž znalost čísla bankovního účtu zaměstnance, aby mohlo docházet k zasílání mzdy či jiného případného plnění.

Zaměstnavatel musí znát také zdravotní pojišťovnu zaměstnance s ohledem na povinnosti uložené mu zákonem č. 48/1997 Sb., o veřejném zdravotním pojištění, nebo mít informace o tom, zda zaměstnanec čerpá určitý typ důchodu. V případě, že zaměstnavatel zajišťuje pro zaměstnance podávání daňových přiznání, bude obhajitelné, aby mu byly poskytovány další osobní údaje zaměstnanců, zejména ty, které jsou nutné pro uplatňování daňových slev (informace o rodinném stavu, o zdravotním stavu, o invaliditě,[425]

[423] Srov. ustanovení § 37 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů.
[424] Srov. stanovení § 15a zákona č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů a ustanovení § 2 zákona č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů.
[425] Tyto informace bude obvykle možné považovat za zvláštní kategorii osobních údajů ve smyslu čl. 9 GDPR. Samostatný výklad k této kategorii osobních údajů je obsažen v následující podkapitole 7.4.

o vyživovaných dětech) nebo pro uplatnění nároku na daňové odpočty (informace o splácení úvěru na koupi nemovitosti, o poskytování různých darů, o čerpání penzijního připojištění apod.).

Zaměstnavatelé také mnohdy požadují informace o předchozí praxi a o dosaženém vzdělání, a to i nad rámec toho, co zaměstnanec uvede ještě jako uchazeč do svého životopisu a dobrovolně poskytne zaměstnavateli. Zpracování takových údajů může být obhajitelné, pokud například zaměstnavatel zaručuje při splnění určité délky praxe či vzdělání kariérní růst nebo přiznává větší odměnu. Využití takových informací by však mělo být omezené, zejména by si zaměstnavatel měl pouze ověřit pravdivost tvrzení zaměstnance, ale už by si neměl pořizovat kopie příslušných diplomů, potvrzení o zaměstnání či jiných dokladů. Opačný postup by totiž odporoval zásadě minimalizace.

Zaměstnavatel bude dále oprávněn znát a zpracovávat osobní údaje nutné pro to, aby mohl plnit svoji povinnost k provádění srážek ze mzdy (včetně případného výkonu rozhodnutí či exekuce). Za určitých okolností mají zaměstnavatelé též nárok na informace o případné jiné výdělečné činnosti (zaměstnání či podnikání), a to pokud by se tato činnost shodovala s předmětem činnosti zaměstnavatele. Taková činnost totiž může být provozována jen se souhlasem zaměstnavatele.[426]

Odhlédneme-li od počáteční fáze pracovněprávního vztahu, platí, že řadu výše zmíněných údajů bude muset zaměstnanec zaměstnavateli oznamovat, i pokud dojde k příslušné skutečnosti až během trvání pracovněprávního vztahu. Obdobně to platí pro případnou změnu jakýchkoliv údajů, ke které dojde během trvání zaměstnání. Platí tak, že zaměstnavatel bude oprávněn zpracovávat i veškeré nové údaje a zaměstnanec bude povinen mu je oznamovat. Může přitom jít o běžné změny týkající se kontaktních údajů (telefonního čísla), adresy bydliště po přestěhování, bankovního účtu, ale i o závažnější záležitosti, jako je nutnost provádět srážky ze mzdy nebo údaje související se zdravotním stavem zaměstnance.

Vedle toho největší rozsah osobních údajů zaměstnance bude generován až při samotném zaměstnání a v souvislosti s ním. Kromě údajů, které jsou imanentní pracovněprávnímu vztahu a budou vznikat vždy (údaje o mzdě, platu či jiné odměně, o pracovní době či době odpočinku, o čerpané dovolené, o době trvání pracovněprávního vztahu, o pracovním zařazení a plnění stanovených úkolů a mnoho dalších), půjde také

[426] Ustanovení § 304 odst. 1 ZPr.

o údaje, které budou generovány jen v návaznosti na určitou právní událost či v závislosti na pracovní pozici zaměstnance a stanovených pracovních povinnostech (údaje o pracovních úrazech a nemocech z povolání, údaje o případné způsobené škodě a způsobech její náhrady, údaje o svěřených pracovních a výrobních prostředcích a způsobu jejich užívání, informace o překážkách v práci, údaje o zvyšování kvalifikace a mnoho dalších). S tím bude souviset také zpracování osobních údajů z kontrol či sledování prováděných zaměstnavatelem, které je velmi citlivé z hlediska ochrany soukromí zaměstnance.[427]

Konečně poslední kategorií potenciálně zpracovávanou zaměstnavatelem jsou osobní údaje související s ukončením pracovněprávního vztahu. Zejména půjde o informace o způsobu ukončení pracovněprávního vztahu (dohoda, výpověď, uplynutí doby trvání atd.) a důvodech takového ukončení. Může se jednat samozřejmě též o informaci, že zaměstnanec zemřel. V takovém případě by však nebylo namístě uplatňovat ochranu osobních údajů dle nařízení GDPR.[428] Půjde také o údaje o případných závazcích mezi zaměstnancem a zaměstnavatelem po skončení pracovního poměru, případně informace související se sporem ohledně neplatného rozvázání pracovního poměru.

Výše uvedené lze shrnout tak, že zaměstnavatelé jsou v závislosti na konkrétních okolnostech oprávněni zpracovávat opravdu značné množství osobních údajů. To s sebou přináší velké nároky na to, aby docházelo k dodržování zákonnosti zpracování osobních údajů, zejména pokud jde o dodržení účelového omezení a nemožnost zaměstnavatelů využívat určité informace pro jiné účely, než pro které byly osobní údaje získány.[429] Autor této práce považuje za stěžejní, aby zaměstnavatelé dokázali pružně reagovat na rozsah jimi zpracovávaných osobních údajů, a to i v návaznosti na zvyšování počtu zaměstnanců spolu s růstem společnosti.

U zaměstnavatele s malým počtem zaměstnanců bude například obhajitelné, aby neexistovalo specializované personální oddělení, aby zaměstnanecké údaje byly zpracovávány bez nebo jen s částečným využitím automatizovaných systémů nebo aby nebyly aplikovány veškeré dostupné nástroje zabezpečení osobních údajů. Naopak u větších zaměstnavatelů či zaměstnavatelů postupně rostoucích toto obvykle možné nebude. Ruku

---

[427] Získávané osobní údaje budou odpovídat prostředkům pro kontroly či sledování zvoleným ze strany zaměstnavatele. K těmto prostředkům viz výklad v podkapitole 8.1.

[428] Srov. preambule (27) nařízení GDPR, podle které platí: *„Toto nařízení se nevztahuje na osobní údaje zesnulých osob.“* Tím však není vyloučeno uplatnění ochrany podle příslušných ustanovení o ochraně osobnosti dle ObčZ.

[429] S výjimkou případů, kdy se bude jednat o zpracování slučitelné s předchozím zpracováním ve smyslu čl. 6 odst. 4 GDPR.

v ruce s tím dochází k vytváření různých interních dokumentů a vystavování nejrůznějších formulářů, kdy je o to více obtížné uhlídat, aby osobní údaje byly zpracovávány skutečně jen v nezbytném rozsahu. Zaměstnavatelé by proto měli pravidelně své interní procesy kontrolovat mimo jiné z tohoto hlediska.

7.4 Zvláštní kategorie osobních údajů

Specifickými osobními údaji, kterým je vhodné věnovat samostatnou podkapitolu, jsou zvláštní kategorie osobních údajů ve smyslu čl. 9 GDPR, dříve též označované jako „citlivé" osobní údaje.[430] Zvláštní kategorií osobních údajů jsou údaje, které *„vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby".*[431] Danou kategorii osobních údajů lze z pohledu autora této práce charakterizovat tak, že s ohledem na jejich znalost by subjekt údajů mohl být snáze diskriminován či jinak znevýhodňován.

Důvodem samostatného výkladu o této kategorii osobních údajů je skutečnost, že kromě toho, že se jedná o relativně úzce vymezený okruh osobních údajů, je možné je zpracovávat jen na základě specifických právních základů definovaných v čl. 9 odst. 2 GDPR (neuplatní se tedy obecná úprava obsažená v čl. 6 odst. 1 GDPR).[432] Jelikož se jedná o relativně úzce vymezený okruh situací, přináší to do praxe celou řadu problémů. Při zpracování zvláštních kategorií osobních údajů totiž především není možné jako právní základy pro zpracování osobních údajů využít (i) nezbytnost zpracování pro splnění smlouvy (čl. 6 odst. 1 písm. b) GDPR) ani (ii) oprávněné zájmy správce či třetí strany (čl. 6 odst. 1 písm. f) GDPR). Právě to je zdrojem zmíněné řady problémů. Za zmínku stojí například otázka zpracování této kategorie osobních údajů v případě poskytování pojistných

[430] V ZOOÚ byly tyto osobní údaje označovány legislativní zkratkou jako citlivé (srov. ustanovení § 4 písm. b) ZOOÚ). Nařízení GDPR sice termín „citlivé" osobní údaje také zná (viz preambule (10) nařízení GDPR), ale jako legislativní zkratku jej pro tuto kategorii osobních údajů nepoužívá.
[431] Viz ustanovení čl. 9 odst. 1 GDPR.
[432] Podle názoru autora této práce není vůbec nutné zabývat se při zpracování zvláštních kategorií osobních údajů ustanovením čl. 6 GDPR. Důvodem je skutečnost, že jednotlivé důvody se překrývají, resp. v čl. 9 odst. 2 GDPR jsou úžeji vymezeny. Odlišně Nulíček, který dovozuje nutnost aplikovat též ustanovení čl. 6 odst. 1 GDPR (Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 164).

produktů, kdy je znalost takových údajů objektivně nezbytná pro řádné posouzení vybraných produktů poskytovaných ze strany pojišťoven (zejména u životního pojištění apod.).[433]

V oblasti zpracování osobních údajů zaměstnanců je situace dále poněkud specifická s ohledem na existenci zvláštních[434] právních základů pro zpracování těchto údajů. Především čl. 9 odst. 2 písm. b) GDPR umožňuje jejich zpracování v případě, že je to *„nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou […]“.*[435] V případech stanovených právními předpisy proto zaměstnavatelé nebudou mít větší problémy s určením právního základu a se zákonností takového zpracování. Půjde především o zpracování informací o zdravotním stavu, které je v určitých situacích zaměstnavatelům uloženo. Výhodou pak také je, že povinnosti mohou zaměstnavatelům v tomto ohledu určovat též kolektivní smlouvy, protože i když se právní základ nezbytnosti pro splnění běžné smlouvy v případě zvláštní kategorie osobních údajů neuplatní, u kolektivních smluv to neplatí.

Druhý specifický právní základ upravující možnost zpracování zvláštní kategorie osobních údajů zaměstnanců nastává v situaci, kdy je zpracování *„nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby […]“.*[436] Správci přitom při zpracování osobních údajů na tomto právním základě musí splnit podmínky dle čl. 9 odst. 3 GDPR a zajistit dodatečné záruky týkající se zabezpečení osobních údajů. S ohledem na obsah tohoto ustanovení je však zřejmé, že se použije především na zpracování osobních údajů ze strany lékařů, nikoliv zaměstnavatelů.

Nebude-li možné aplikovat ani jeden ze dvou výše zmíněných právních základů dle čl. 9 odst. 2 GDPR, bude nutné v témže ustanovení hledat jiný právní základ, což bude v určitých případech nevyhnutelné. Nejčastěji se bude pravděpodobně jednat o právní základ, kdy je zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků ve smyslu čl. 9 odst. 2 písm. f) GDPR. Naopak za obvykle nevhodný bude nutné považovat

---

[433] V praxi bývá takovéto zpracování realizováno obvykle na základě výslovného souhlasu (který však autor této práce s ohledem na jeho odvolatelnost nepovažuje za vhodný právní základ), nebo s odkazem na nezbytnost zpracování pro určení, výkon nebo obhajobu právních nároků ve smyslu čl. 9 odst. 2 písm. f) GDPR.
[434] Vyloučit samozřejmě nelze ani využití jiných právních základů ve smyslu čl. 9 odst. 2 GDPR. Cílem je však poukázat na ty, které jsou specifické pro zpracování zvláštních kategorií osobních údajů zaměstnanců.
[435] Čl. 9 odst. 2 písm. b) GDPR.
[436] Čl. 9 odst. 2 písm. h) GDPR.

výslovný souhlas zaměstnance dle čl. 9 odst. 2 písm. a) GDPR s ohledem na zaměstnancovo slabší postavení a spornou svobodnost udělení takového souhlasu. Využití jednotlivých právních základů je dále zkoumáno v návaznosti na jednotlivé zvláštní kategorie osobních údajů.

7.4.1 Informace o zdravotním stavu

Pokud jde o jednotlivé zvláštní kategorie osobních údajů, se kterými se budou zaměstnavatelé setkávat, jsou to zejména o údaje o zdravotním stavu. Bude-li se jednat o situace, kdy je jejich zpracování uloženo zákonem (informace o zdravotní způsobilosti zaměstnance pro výkon práce, zaměstnání osob se změněnou pracovní schopností, zpracování informací o pracovním úrazu apod.), nebude určení zákonnosti takového zpracování činit větší obtíže.

Obtížnější situace může nastat, pokud vazba na konkrétní zákonnou povinnost není jednoznačná. Navíc platí, že pojem údaje o zdravotním stavu je třeba vykládat spíše široce. Ačkoliv definice údajů o zdravotním stavu obsažená v čl. 4 bodu 15) je relativně stručná,[437] lze vyjít z výkladu podaného v preambuli GDPR, kde se mimo jiné uvádí: *„Mezi osobní údaje o zdravotním stavu by měly být zahrnuty veškeré údaje související se zdravotním stavem subjektu údajů, které vypovídají o minulém, současném či budoucím tělesném nebo duševním zdraví subjektu údajů. To zahrnuje informace o dané fyzické osobě shromážděné v průběhu registrace […], číslo, symbol nebo specifický údaj přiřazený fyzické osobě […], informace získané během provádění testů nebo vyšetřování části těla nebo tělesných látek, včetně z genetických údajů a biologických vzorků, a jakékoliv informace například o nemoci, postižení, riziku onemocnění, anamnéze, klinické léčbě nebo fyziologickém či biomedicínském stavu subjektu údajů nezávisle na jejich původu […]“.*[438]

SDEU tak například dovodil, že za údaj o zdravotním stavu je nutné považovat též informaci, že se určitá osoba zranila na noze a čerpá částečné volno z důvodu nemoci.[439] Za vhodný právní základ bude možné považovat nezbytnost zpracování pro určení, výkon nebo obhajobu právních nároků,[440] případně zpracování osobních údajů zjevně zveřejněných

---

[437] Podle tohoto ustanovení se údaji o zdravotním stavu rozumí „*osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.“*

[438] Viz preambule (35) GDPR.

[439] Srov. rozhodnutí SDEU ze dne 6. listopadu 2003, C-101/01, ve věci Bodil Lindqvist.

[440] Ve smyslu čl. 9 odst. 2 písm. f) GDPR.

subjektem údajů (bude-li to relevantní).[441] Naopak obecně nevhodným právním základem bude výslovný souhlas zaměstnance s takovým zpracováním.[442] Nenalezne-li zaměstnavatel jiný vhodný právní základ, bude muset zpracování daných osobních údajů neprodleně ukončit, resp. je zpracovávat jen v takovém rozsahu, v jakém mu to ukládá zákon (či kolektivní smlouva).

7.4.2 Členství v odborové organizaci

Další zvláštní kategorií osobních údajů, se kterou se budou zaměstnavatelé setkávat, je údaj o členství zaměstnance v odborech. ZPr v mnohých případech zaměstnavatelům ukládá určité povinnosti v souvislosti s tím, že zaměstnanec je členem odborové organizace, respektive tuto znalost u zaměstnavatele implicitně předpokládá. Jde například o situaci, kdy si zaměstnavatel musí vyžádat předchozí souhlas k výpovědi dané členu odborové organizace ve smyslu § 61 ZPr, kdy je umožněno provádění srážek ze mzdy k úhradě členských příspěvků zaměstnance dle § 146 písm. c) ZPr, uplatnění částky zaplacených odborových příspěvků jako odečitatelné položky podle zákona č. 586/1992 Sb., o daních z příjmu,[443] nebo obecně v situacích, kdy je zaměstnavatel povinen určité skutečnosti s odborovou organizací projednávat nebo ji informovat.

Oprávnění zaměstnavatele ke zpracování údaje o členství v odborové organizace sice v těchto situacích sice není explicitně vyjádřeno, i přesto se autor této práce domnívá, že je nutné dovodit oprávněnost zaměstnavatele ke zpracování těchto osobních údajů s odkazem na zmiňovaný zvláštní právních základ podle ustanovení § 9 odst. 2 písm. b) GDPR. O to bude však důležitější, aby zaměstnavatel dané údaje zpracovával striktně pro splnění stanovených povinností a nevyužíval je pro žádné jiné účely (například plánování organizačních změn, propouštění zaměstnanců atd.). Zpracování pro takové účely by bylo bez dalšího (například bez existence souhlasu) nutné považovat za nezákonné.

---

[441] Ve smyslu čl. 9 odst. 2 písm. e) GDPR.
[442] Ve smyslu čl. 9 odst. 2 písm. a) GDPR.
[443] Za nesystematický a překonaný považuje autor této práce názor vyjádřený Úřadem pro ochranu osobních údajů, že v souvislosti s prováděním dohody o srážkách ze mzdy nepotřebuje zaměstnavatel zpracovávat citlivý údaj vypovídající o členství zaměstnance v odborové organizaci, neboť tento byl dovozován účelově zejména s ohledem na oznamovací povinnost dle § 16 ZOOÚ (srov. stanovisko ÚOOÚ č. 2/2001: *Zpracování citlivého osobního údaje o členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací*. Říjen 2001, aktualizováno červenec 2006, červen 2007, revize srpen 2009).

7.4.3 Odsouzení za trestný čin

Zaměstnavatelé se dále za určitých okolností mohou dostat k informaci o tom, zda zaměstnanec spáchal určitý trestný čin a byl za něj odsouzen. Tato informace nicméně již není řazena do stejné kategorie jako ostatní zvláštní kategorie osobních údajů dle čl. 9 GDPR (na rozdíl od řazení mezi citlivé osobní údaje v rámci ZOOÚ), nýbrž je specificky upravena v rámci samostatného čl. 10 GDPR. Zpracování těchto informací je podle tohoto ustanovení možné jen v situacích pod dozorem orgánu veřejné moci, pokud je to oprávněné dle právních předpisů poskytujících vhodné záruky nebo pokud jde o práva a svobody subjektů údajů.[444]

Zaměstnavatelé se budou s těmito údaji setkávat zejména u uchazečů o zaměstnání a při náboru nových zaměstnanců. Za určitých okolností totiž mohou zaměstnavatelé důvodně požadovat, aby jim zaměstnanci prokazovali, že nebyli odsouzeni pro žádný trestný čin, a to předložením výpisu z rejstříku trestů. Ve smyslu příslušných právních předpisů se jedná o prokazování tzv. bezúhonnosti.[445] Musí jít však o výjimečně situace ve smyslu § 316 odst. 4 ZPr. K otázce požadování výpisu z rejstříku trestů zaměstnanců se též vyjádřil ÚOOÚ, který uvedl, že *„výpis z rejstříku trestů, který dokládá beztrestnost, není citlivým osobním údajem o „odsouzení za trestný čin“ ve smyslu § 4 písm. b) zákona o ochraně osobních údajů“*.[446] S ohledem na obdobnost příslušných pojmů obsažených v GDPR a ZOOÚ tak lze dojít k závěru, že výpis z rejstříku trestů neobsahující žádné údaje odsouzení nepodléhá režimu dle čl. 10 GDPR.[447]

Mnohdy se však zaměstnavatelé dostanou též nepřímo či nechtěně k informacím o určitém odsouzení zaměstnanců či uchazečů o zaměstnání (které není rozhodné pro dané zaměstnání). V takovém případě už o zpracování odsouzení za trestný čin nepochybně jde. Zaměstnavatel musí s touto možností počítat a být na ni připraven. Kromě již zmiňované možnosti požadovat doložení bezúhonnosti jen ve výjimečných případech (ve smyslu § 316 odst. 4 ZPr) pak z toho může pro zaměstnavatele vyplývat celá řada dalších povinností, jako je omezení možnosti zpracovávat takové údaje pro jiné účely (čl. 6 odst. 4 GDPR), povinnost provést posouzení vlivu (čl. 35 GDPR) či povinnost jmenovat pověřence pro ochranu

---

[444] Viz čl. 10 GDPR.
[445] Blíže k termínu bezúhonnost srov. Mráz, M. *Bezúhonnost v právním řádu České republiky*. © EPRAVO.CZ. Publikováno dne 1. prosince 2015 [online]. [cit. 2019-04-02]. Dostupné z: https://www.epravo.cz/top/clanky/bezuhonnost-v-pravnim-radu-ceske-republiky-99570.html
[446] Stanovisko ÚOOÚ č. 6/2012: *Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů*. Březen 2012, poslední revize duben 2013.
[447] Shodně Nulíček in Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 170.

osobních údajů (čl. 37 GDPR). Pro tyto situace lze proto obecně zaměstnavatelům doporučit tyto údaje nijak nezpracovávat a pouze si poznamenávat, zda došlo či nedošlo k doložení bezúhonnosti.

7.4.4 Biometrické údaje

Jednou z dalších ze zvláštních kategorií osobních údajů, se kterou zaměstnavatelé přicházejí do kontaktu, jsou biometrické údaje. Biometrickými údaji se ve smyslu čl. 4 bodu 14) GDPR rozumí *„osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“*. V praxi na pracovišti se může jednat nejčastěji o otisky prstů, záznam hlasu či scan oční duhovky využívaný pro přístupové systémy, ale může jít i o bližší informace o podobizně zaměstnance, o specifických prvcích chůze (které mohou být využívány pro účely ostrahy různých objektů) nebo o rukopisu zaměstnance.

Je nutné podotknout, že vymezení určitého údaje jako biometrického ve smyslu čl. 9 GDPR nebude vždy snadné. Zejména u podobizny nebo fotografie platí, že ne každé zpracování fotografie by mělo být považováno za zpracování ve smyslu zvláštních kategorií osobních údajů. Fotografie by měla být za biometrický údaj považována pouze v případech, kdy je zpracovávána zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby.[448] Fotografie pořízená na průkaz zaměstnance by tedy obecně neměla být považována za biometrický údaj ve smyslu čl. 9 GDPR.

Pokud jde o podmínky, za kterých mohou zaměstnavatelé biometrické osobní údaje zpracovávat, jen nutné vyjít z účelů jejich zpracování. Jak bylo naznačeno, bude se nejčastěji jednat o (i) docházkové systémy, (ii) systémy umožňující přístup či (iii) jiné bezpečnostní systémy (monitorovací či sledovací).

Pro přístupové systémy bude ve specifických případech možné dovozovat určité zákonné požadavky na zajištění odpovídajícího zabezpečení. Takto je možné zmínit povinnost stanovenou § 11 a § 13 vyhlášky č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu. Obdobné povinnosti týkající se fyzické bezpečnosti, ačkoliv biometrika explicitně zmíněna není, jsou obsaženy v 24 a násl. zákona č. 412/2005 Sb., o ochraně utajovaných informací, zejména jde o povinnost zajistit systémy pro kontrolu vstupů ve smyslu § 30 odst. 1 tohoto zákona. Za zmínku stojí skutečnost, že využití

[448] Viz preambule (51) nařízení GDPR.

výslovného souhlasu jako právního základu pro zpracování těchto údajů ve smyslu čl. 9 odst. 2 písm. a) může fungovat (může být zákonné) za předpokladu, že zaměstnanec bude mít k dané volbě alternativu. Například bude moci využívat osobní kartu, heslo či jiný ověřovací prvek. Pak bude tedy možné aplikovat využití biometrických osobních údajů pro přístupové systémy i v situacích, kdy to nebude uloženo právním předpisem.[449]

U docházkových systémů je situace složitější. ÚOOÚ obecně zastává postoj, že zpracování takovýchto osobních údajů pro vedení docházky je nepřípustné.[450] V právních předpisech neexistuje pro tento účel specifické zmocnění. S ohledem na explicitní zákaz použití biometrického údaje pro účely jednoznačné identifikace fyzické osoby, jak je dnes obsažený v GDPR, by nebylo ani možné uvažovat o situaci, kdy by biometrický údaj byl ihned po přečtení převeden na jinou, nikoliv biometrickou informaci, s kterou by bylo pro účely docházky pracováno (tato možnost byla dovozována před účinností GDPR).

Autor této práce se nicméně domnívá, že i přesto by pro docházkové systémy bylo možné využít biometrické osobní údaje, pokud k tomu bude zaměstnancem udělen výslovný souhlas. Samozřejmostí i zde musí být to, že půjde o skutečně platně udělený souhlas (například, že zaměstnanec má alternativu k biometrice) a že je zpracování omezeno z věcného (rozsah) i časového (doba) hlediska na nezbytné minimum. Odlišný pohled zastává ÚOOÚ, který zcela odmítá využití biometrických údajů pro docházkové systémy, a to i pokud by k tomu byl ze strany subjektu údajů udělen výslovný souhlas, jako důvod uvádí, že zpracování neodpovídá stanovenému účelu a nejde o nezbytný rozsah.[451] Podle názoru autora této práce však zpracování biometrického údaje účelově dává smysl i pro docházkové systémy, neboť jiné systémy (například karty) se dají obvykle relativně snadno obelstít (například pouhým předáním jiné osobě) a zaměstnavatelé jsou poté nuceni sahat k závažnějším zpracováním pomocí kamer, aby si v případě pochybností mohli ověřit, že zaměstnanec do práce skutečně dorazil. Pokud jde o argument ÚOOÚ týkající se nadbytečného rozsahu, k tomu lze uvést, že ten je do určité míry vždy překročen u souhlasového zpracování, ale právě protože se jedná o souhlasové zpracování, je nutné posuzovat nezbytnost rozsahu méně přísným měřítkem. Ochrana subjektu údajů je zde

[449] Obdobné závěry vyplývají též ze stanoviska ÚOOÚ č. 1/2017: *Biometrická identifikace nebo autentizace zaměstnanců*. Červen 2017.
[450] Tamtéž.
[451] Tamtéž.

zajištěna primárně odvolatelností souhlasu, jejímž využitím může subjekt údajů sám kdykoliv rozhodnout o ukončení zpracování.

Posledním případem, kdy může přicházet do úvahy využití biometrických údajů a který stojí z hlediska praxe za zmínku, je zpracování biometrických údajů při monitorování či sledování prostřednictvím kamer či jiných obdobných nástrojů, které umí zachytit a vyhodnocovat biometrické prvky a které bývají obvykle využívány pro účely zabezpečení různých objektů, včetně pracovišť. Bude se jednat především o specifické prvky chůze a pohybů osob zachycených na kamerách, rysy obličeje apod. Moderní systémy dokážou tyto údaje vyhodnocovat a určit, zda se na daném záběru nevyskytuje osoba, která se tam vyskytovat nemá či nesmí. To samo sebou přináší nutnost zpracování odpovídajících biometrických údajů osoby, která se na daném místě vyskytovat má. Odpověď na možnost zpracování těchto údajů bude obdobná jako u systémů monitorujících přístup. Tyto údaje tedy bude možné zpracovávat, pokud bude existovat specifické zákonné zmocnění k využití takovýchto osobních údajů pro zajištění fyzické ostrahy. Naopak ale v tomto případě nebude připadat do úvahy možnost využití výslovného souhlasu, neboť v tomto případě pro zaměstnance nebude nikdy existovat možnost neudělení souhlasu, a tudíž by vyžadování a udělení souhlasu bylo neplatné. To je navíc na pracovišti umocněno specifičností vztahu zaměstnance a zaměstnavatele a dále ustanovením § 316 ZPr omezujícím možnost sledování zaměstnanců.

7.4.5 Shrnutí

Výše zmíněné zvláštní kategorie osobních údajů nejsou jediné, se kterými se zaměstnavatelé mohou setkat. Do úvahy mohou dále připadat například údaje, které vypovídají o politických názorech či náboženském vyznání. Obvykle náhodně se zaměstnavatelé mohou setkat též se zbývajícími ze zvláštních kategorií osobních údajů. Mohou samozřejmě nastat situace, kdy bude zpracování takovýchto údajů odůvodnitelné. Například informace o politických názorech v případě různých politických stran a hnutí, či informace o náboženském vyznání v případě církví a náboženských společností. Zpracování takových údajů by však běžně nemělo vyvolávat příliš otázek, a to i s ohledem na specifickou regulaci obsaženou v ustanovení § 316 odst. 4 ZPr, § 12 odst. 2 ZoZ či v antidiskriminačním zákoně.

Důležitějším jsou proto výše v této práci zmiňované a do větší hloubky analyzované zvláštní kategorie osobních údajů, s jejichž zpracováním se bude možné v praxi setkávat

častěji. Přes snahu objasnit v této práci veškeré možné případy zpracování takových údajů, zůstávají při určování zákonnosti jejich zpracování některé otevřené otázky. V každém případě je zřejmé, že zaměstnavatelé by ke zpracování takových osobních údajů měli přistupovat zvlášť obezřetně a striktně dodržovat zásadu účelového omezení a nevyužívat tyto informace pro jiné své potřeby. Právní úprava obsažená v GDPR není (s ohledem na svou obecnost) v otázce určování právních základů pro zpracování zvláštních kategorií osobních údajů zaměstnanců příliš jednoznačná a nenasedá na některé specifické aspekty při jejich zpracování. Do větší míry se s tím však lze vypořádat výkladem a nalézt odpovídající právní základ, kdy je možné takové údaje zpracovávat.

Na závěr této podkapitoly stojí za zmínku skutečnost, že zpracování zvláštních kategorií osobních údajů je podle GDPR v případě zaměstnanců možné také s odkazem na nezbytnost plnění kolektivní smlouvy. Takovéto záležitosti se však prozatím kolektivním smlouvám vyhýbají. Uvidíme, co přinese další vývoj a zda se tato situace do budoucna nezmění. Na druhou stranu by motivem pro změnu v tomto ohledu měla být spíše skutečná snaha o oslovení těchto otázek v kolektivních smlouvách, a nikoliv snaha o odstraňování některých legislativních nedostatků.

7.5 Omezení uložení

Další z důležitých zásad, kterou se musí řídit každé zpracování osobních údajů, je zásada omezení uložení. V rámci čl. 5 GDPR je tato zásada vymezena tak, že *„osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely […]“*.[452] Z uvedeného je zřejmé, že tato zásada se týká doby, po kterou je možné osobní údaje zpracovávat, a jejím obsahem je povinnost osobní údaje po uplynutí stanovené doby vymazat, případně alespoň anonymizovat.[453]

---

[452] Čl. 5 odst. 1 písm. e) GDPR.

[453] Pokud dojde k anonymizaci osobních údajů, platí, že se už nejedná o osobní údaje ale o údaje anonymizované, tj. informace, které není možné (přímo či nepřímo) vztáhnout žádné fyzické osobě. Nařízení GDPR v preambuli (26) jasně uvádí, že na takové anonymizované údaje se nevztahují zásady ochrany osobních údajů, tedy ochrana poskytovaná nařízením GDPR. Pokud jde o otázku toho, kdy a jak lze docílit anonymizace, nejedná se obvykle o zcela jednoduchý proces, jelikož prosté odstranění identifikačních a kontaktních údajů nebude k anonymizaci dostačovat, když kombinace jiných informací často má potenciál určit jednu konkrétní fyzickou osobu. Blíže se k procesu anonymizace vyjádřila WP29 ve stanovisku č. 5/2014: K technikám anonymizace (v originále: *opinion 5/2014 on Anonymisation Techniques*). (WP216), ze dne 10. dubna 2014.

Určení doby zpracování a okamžiku, kdy je možné, respektive nutné, osobní údaje vymazat, není obvykle jednoduché. Předně platí, že osobní údaje jsou často zpracovávány pro více účelů, přičemž doba zpracování jednotlivých účelů se obvykle liší. Pokud uplyne doba zpracování jednoho z účelů zpracování, ale bude existovat jiný účel, osobní údaje samozřejmě vymazány být nemusí. Toto je však nutné zkoumat zvlášť k jednotlivým osobním údajům. Proto se může stát, že po uplynutí doby zpracování bude nutné určité informace odstranit, ale určité bude možné ponechat nadále. Dokud tedy k určitému osobnímu údaji bude existovat alespoň jeden účel zpracování, nebude nutné takový osobní údaj vymazat. Naopak pokud byť k jednomu určitému osobnímu údaji již žádný účel (a právní základ) existovat nebude, bude jej nutné odstranit.[454] Správce má zároveň s ohledem na zásadu minimalizace osobních údajů povinnost toto posuzovat průběžně. Ve vztahu mezi zaměstnavatelem a zaměstnancem přitom tato potřeba bude vznikat již v průběhu trvání pracovního poměru, nikoliv vždy až po jeho skončení (například staré adresní a kontaktní údaje zaměstnance, které bude zaměstnavatel povinen odstranit v případě jejich změny).

Další komplikací při dodržování této zásady je přesné určení doby, po kterou mohou být osobní údaje zpracovávány. Nařízení GDPR nepřímo uznává, že dobu nebude vždy možné přesně určit, a to v rámci ustanovení, kterým je uloženo subjekty údajů o zpracování informovat. Podle čl. 13 odst. 2 písm. a) GDPR je tak správce povinen poskytnout informace o době *„po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby“*. Tím je zejména připuštěno navázat dobu zpracování na jiné právní události či jednání. U zaměstnanců může příkladem doba trvání pracovní smlouvy či doba vedení sporu se zaměstnancem. Je jasné, že u obou těchto příkladů není možné předem jasně určit konkrétní dobu, kdy bude zpracování ukončeno, ale zároveň takto určená doba nebude připouštět pochybnosti, jakmile dojde k jejímu uplynutí. Ani takové určení doby nemusí být vždy možné. Tuto problematiku vystihuje Nulíček, který uvádí, že *„doba nicméně nemůže být stanovena jako doba zcela neurčitá, vždy bude objektivně posuzováno, zda doba uchování nepřekročila dobu nezbytnou k naplnění účelu zpracování“*.[455]

---

[454] Věc může být navíc komplikovaná tím, že určité osobní údaje k vymazání mohou být obsaženy na určité listině spolu s jinými osobními údaji, na které zaměstnavatel nárok má i nadále. *Stricto sensu* by pak měla být odstraněna jen příslušná část osobních údajů, například jejich začerněním. V praxi však bude splnění této povinnosti s ohledem na obtížnost objektivně nerealizovatelné. Podle názoru autora této práce by proto na této povinnosti nemělo být důsledně trváno.

[455] Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 114.

ÚOOÚ jako příklad nevhodného určení doby dále uvádí odkazování se na obecné promlčecí či prekluzivní lhůty, pokud již neprobíhá např. soudní či jiné řízení anebo pokud není důvodné takové řízení předpokládat.[456] S tímto lze podle názoru autora této práce polemizovat. Obzvláště u větších zaměstnavatelů může být nemožné předem obecně určovat, že po ukončení pracovního poměru se zaměstnancem žádný spor nehrozí. Ač půjde spíše o menší počet případů, může se stát, že spor bude zahájen i s odstupem určité doby (na což mohou mít vliv i interní organizační změny u zaměstnavatele, např. změna vedení). Zaměstnavatel by se přitom výmazem osobních údajů (a související dokumentace) v podstatě zbavil možnosti efektivně se proti nárokům zaměstnance bránit. Takovým postupem by se zaměstnavatel, resp. osoby jednající v jeho čele mohly dopustit porušení jednat s odpovídající úrovní péče (odborné péče, péče řádného hospodáře apod.) a výsledný stav by mohl být vymáhán společností na jejich úkor. Autor této práce se tedy domnívá, že obecně nelze vylučovat vymezení doby zpracování s odkazem na běh promlčecích lhůt. Nemělo by však docházet k nadužívání tohoto institutu v situacích, kdy lze dobu snadno určit podle jiných kritérií.

Bez ohledu na uvedené platí, že zaměstnavatel by měl existenci správnosti určení doby pro jednotlivá zpracování průběžně monitorovat. Může se totiž z různých důvodů stát, že předem obecně určená doba uplyne dříve a osobní údaje bude skutečně možné a nutné dříve vymazat. Příkladem může být situace, kdy budou osobní údaje zpracovávány v evidenci uchazečů o zaměstnání na základě jeho souhlasu, avšak z obecně zřejmých okolností již bude patrné, že uchazeč již o zaměstnání nemá zájem. Může jít i o situaci, kdy bude spor s bývalým zaměstnancem ukončen dohodou o narovnání (aniž by toto mělo samozřejmě vliv na zákonem stanovené doby, po které je nutné vybrané osobní údaje zpracovávat).

7.5.1 Doba zpracování osobních údajů zaměstnanců

Záměrem tohoto bodu je analyzovat v praxi nejčastější případy zpracování osobních údajů zaměstnavateli ve vazbě na dobu zpracování takových osobních údajů. Jak bylo uvedeno výše, při definování doby je potřeba vycházet z účelu zpracování. Ty byly blíže popsány v podkapitole 6.2.

---

[456] ÚOOÚ: *Ke zpracování osobních údajů bývalých zaměstnanců*. Závěry z rozhodnutí ÚOOÚ sp. zn. č. j. SKO-2077/07. Vytvořeno dne 21. března 2013 [online]. [cit. 2019-03-25]. Dostupné z: https://www.uoou.cz/ke-zpracovani-osobnich-udaju-bývalych-zamestnancu/d-1585/p1=1279

U uchazečů o zaměstnání je zřejmé, že doba zpracování by neměla překročit dobu vedení výběrového řízení a určitou bezprostředně navazující dobu poté. To nebude platit, pokud uchazeč o zaměstnání udělí souhlas s dalším zpracováním, v rámci kterého by byla jasně stanovena doba dalšího zpracování. U zaměstnanců samotných bude vždy hodně záležet na konkrétním účelu zpracování. Půjde-li o účel, který bude postaven na právním základu splnění smlouvy ve smyslu čl. 6 odst. 1 písm. b) GDPR, nabízí se dobu zpracování takových osobních údajů navázat na dobu trvání pracovní smlouvy a dále na přiměřenou dobu, po kterou může být relevantní údaje mít. Taková relevantní doba může být podle názoru autora této práce určena s odkazem na již zmiňované promlčecí lhůty, zejména tedy lze vyjít z obecné tříleté promlčecí lhůty. Je však nutné poznamenat, že v tomto případě, když už nejsou osobní údaje skutečně nutné ke splnění smlouvy, jejíž je zaměstnanec stranou, ale jde o jiný účel (zejména ochrana práv zaměstnavatele), se původní účel zpracování údajů transformuje a bude navázán na právní základ ochrany oprávněných zájmů zaměstnavatele dle čl. 6 odst. 1 písm. f) GDPR. Otázka slučitelnosti účelů zpracování dle čl. 6 odst. 4 GDPR by v těchto případech neměla činit žádné obtíže.

Půjde-li o účely, které se budou vázat na splnění zákonem stanovených povinností ve smyslu čl. 6 odst. 1 písm. c) GDPR, je situace o poznání komplikovanější. Řada předpisů zmiňovaných v bodě 6.2.1 určuje vlastní dobu, po kterou je nutné osobní údaje uchovávat, řada předpisů však žádnou dobu neurčuje. Konkrétně určenou dobu lze nalézt zejména v zákoně č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, který stanoví tříletou dobu uchování pro evidenčních listů a záznamů o skutečnostech vedených v příslušné evidenci, resp. dobu desetiletou, pokud jde o některé vybrané údaje v příslušné evidenci, ale dokonce až třicetiletou dobu pro mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění.[457] Dalšími zákony jsou zákon č. 187/2006 Sb., o nemocenském pojištění, který zaměstnavateli ukládá příslušné záznamy uchovávat po dobu 10 kalendářních roků následujících po roce, kterého se týkají, nestanoví-li jiné právní předpisy delší uschovací dobu,[458] zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení, který ukládá povinnost plátcům pojistného uschovávat účetní záznamy o údajích potřebných pro stanovení a odvody pojistného po dobu 10 kalendářních roků po

[457] Viz. § 35a odst. 4 citovaného zákona.
[458] Za příslušné záznamy se přitom vždy považují doklady o druhu, vzniku a skončení pracovního vztahu a záznamy o evidenci docházky do práce, včetně doby pracovního volna bez náhrady příjmu; srov. § 96 citovaného zákona.

roce, kterého se týkají,[459] nebo zákon č. 435/2004 Sb., o zaměstnanosti, který mimo jiné ukládá uchovávat kopie dokladů prokazujících oprávněnost pobytu cizince na území České republiky, a to po dobu trvání zaměstnání a dobu 3 let od skončení zaměstnávání tohoto cizince.[460]

Budou-li osobní údaje obsaženy v účetních dokladech, účetních knihách, odpisových plánech, inventurních soupisech, účetních záznamech apod., bude rovněž nutné dodržovat povinnosti stanovené zákonem č. 563/1991 Sb., o účetnictví, a uchovávat je po dobu 5 let počínajících koncem účetního období, kterého se týkají, resp. 10 let v případě, že se bude jednat o účetní závěrku nebo výroční zprávu společnosti.[461] Rovněž pokud bude zaměstnavatel zpracovatelem daňových přiznání svých zaměstnanců, bude muset po stanovenou dobu uchovávat příslušné podklady. Tato doba bude odpovídat lhůtě pro stanovení daně ve smyslu § 148 zákona č. 280/2009 Sb., daňový řád, a může činit až 10 let.[462]

Samotný zákoník práce, který také v mnoha případech ukládá zaměstnavatelům vést různé údaje o zaměstnancích (zejména vedení osobního spisu, informace na úseku BOZP a ve vztahu k pracovním úrazům), žádné vodítko, jak určit nezbytnou dobu pro zpracování, nepodává. Aniž by to mělo být považováno za obecně platné pravidlo, lze nicméně konstatovat, že takové osobní údaje budou zaměstnavatelé oprávnění zpracovávat po dobu trvání pracovněprávního vztahu a určitou dobu poté (s odkazem na běh promlčecích lhůt nebo s odkazem na plnění vybraných výše uvedených zákonných povinností).

Pokud bude u zaměstnavatele docházet ke zpracování osobních údajů zaměstnanců s odkazem na oprávněný zájem ve smyslu čl. 6 odst. 1 písm. f) GDPR, zaměstnavatelé budou muset v závislosti na každém konkrétním účelu posuzovat, co je nezbytná doba zpracování pro naplnění daného účelu. Rozhodně platí, že bude diametrálně odlišná doba v situacích, kdy s odkazem na tento právní základ budou provádět sledování či monitorování zaměstnanců, zejména kamerovými systémy, kde budou moci být záznamy uchovávány řádově jednotky dnů, a naopak kdy si zaměstnavatel některé osobní údaje obsažené v dokumentech ponechá po skončení pracovního poměru pro případnou obranu ve sporu se zaměstnancem, pokud by takový spor vznikl.

---

[459] Ustanovení § 22c citovaného zákona.
[460] Ustanovení § 102 odst. 3 citovaného zákona.
[461] Ustanovení § 31 citovaného zákona.
[462] Ve smyslu § 148 odst. 5 citovaného zákona

Asi nejméně obtíží přináší zpracování osobních údajů s odkazem na udělený souhlas ve smyslu čl. 6 odst. 1 písm. a) GDPR. Na druhou stranu však neplatí, že by v těchto případech bylo v praxi postupováno obvykle v souladu s požadavky na zákonné zpracování osobních údajů. Jak bylo uvedeno výše v bodě 6.2.4, využitelnost souhlasového zpracování je u zaměstnavatele značně omezena. Zaměstnavatel bude muset vždy předem určit jasnou dobu platnosti takového souhlasu, přičemž bude záviset na souvislostech a účelech takového souhlasu. WP29 v této souvislosti jako osvědčený postup doporučovala, aby byl souhlas ve vhodných intervalech obnovován, aby měl dotčený subjekt i nadále všechny aktuální informace o daném zpracování.[463] Autor této práce se nicméně domnívá, že není nutné toto vztahovat též na vztah mezi zaměstnancem a zaměstnavatelem, který na rozdíl od jiných vztahů mezi správcem a subjektem údajů vykazuje určitou blízkost a trvalost, alespoň po dobu trvání pracovního poměru. Rovněž tedy podle názoru autora této práce není vyloučené, aby byla doba udělení souhlasu navázána na dobu trvání pracovního poměru a dále na přiměřenou dobu poté (například jeden rok).

7.6 Zpřístupňování údajů třetím osobám

Zaměstnavatel při zpracování osobních údajů svých zaměstnanců vystupuje jako správce, určuje účely a prostředky zpracování osobních údajů a je plně za zpracování odpovědný. V některých situacích bude však zaměstnavatel osobní údaje předávat třetím stranám, které také mohou osobní údaje v určitém rozsahu zpracovávat a které mohou vystupovat v pozici samostatného správce nebo i zpracovatele. Záměrem této podkapitoly je poskytnout přehled takovýchto situací a posoudit podmínky, za kterých takové předávání osobních údajů může probíhat.

7.6.1 Předávání jiným správcům

Nezpochybnitelným případem, kdy bude docházet k předávání osobních údajů zaměstnanců bez splnění dalších podmínek, jsou situace, kdy to zaměstnavateli ukládá zákon. To se bude týkat zejména předávání osobních údajů správě sociálního zabezpečení, veřejným zdravotním pojišťovnám, finančním úřadům a dalším orgánům v souvislosti s plněním povinností vyplývajících z pracovního poměru zaměstnance (úřad práce, inspekce práce apod.). Pod plnění zákonných povinností bude spadat též předávání osobních údajů

[463] WP29: *Pokyny pro souhlas podle nařízení 2016/679*. (WP 259 rev. 01), vydané dne 28. listopadu 2017, v revidovaném znění ze dne 10. dubna 2018, s. 22.

soudům, exekutorům, orgánům činným v trestním řízení či jiným orgánům veřejné moci v souvislosti s výkonem jim svěřené pravomoci. Zčásti ještě plněním zákonných povinností, byť zčásti i plněním smluvních závazků zaměstnavatele bude předávání osobních údajů mezi zaměstnavatelem a poskytovatelem pracovnělékařských služeb či jinými subjekty v souvislosti s pracovními úrazy (například poskytovatel BOZP či pojišťovny).

Spíše již s odkazem na plnění smluvních závazků zaměstnavatele bude probíhat předávání osobních údajů zaměstnanců poskytovatelům nejrůznějších benefitů, na kterých se zaměstnavatel a zaměstnanec dohodli, resp. které je zaměstnavatel povinen zajišťovat podle vnitřního předpisu, kolektivní smlouvy či na jiném obdobném základě.[464] Půjde zejména o předávání poskytovatelům benefitů a školení, pořadatelům událostí pořádaných zaměstnavatelem, pojišťovnám, penzijním společnostem, společnostem poskytující stravovací či sportovní služby jako zaměstnanecký benefit, poskytovatelům služeb odborného vzdělávání, poskytovatelům telekomunikačních služeb apod. Jelikož už obvykle nepůjde o předávání uložené zákonem, zaměstnavatel by měl ve smyslu zásady odpovědnosti za zpracování (čl. 5 odst. 2 GDPR) smluvně i technicky zajistit, aby předávání bylo prováděno řádně. Zejména by měl alespoň rámcově s třetí stranou smluvně upravit, proč a jakým způsobem bude docházet k předávání osobních údajů a jaký bude způsob takového předávání. Spolu s tím jsou samozřejmě zaměstnavatel i třetí strana povinni zajistit, aby takové předávání probíhalo dostatečně zabezpečeným způsobem.

Předávání osobních údajů zaměstnanců třetím osobám je samozřejmě možné též v situaci, kdy k tomu zaměstnanci udělí souhlas a kdy budou o podmínkách (zejména o účelech) takového předání řádně informováni. Může se jednat například o situace, kdy zaměstnavatel jako zprostředkovatel nabídne zaměstnancům určitý produkt nebo službu třetí strany. V případě, že zaměstnanci o takový produkt či službu projeví zájem, předá následně zaměstnavatel osobní údaje zaměstnanců příslušné třetí straně. Výše zmíněné smluvní a technické podmínky pro předávání osobních údajů, které by zaměstnavatel měl zajistit, zde platí obdobně.

Spíše okrajová bude situace, kdy bude možné zaměstnavatele považovat za společného správce se třetí osobou ve smyslu čl. 26 GDPR. Jak bylo ale uvedeno v bodě 6.1.2, i k těmto situacím může docházet. Podle WP29 by mohl být zaměstnavatel společným

---

[464] Shodný názor zastává též ÚOOÚ, srov. ÚOOÚ: Sekce: často kladené dotazy. *Zaměstnavatelé*. *Jaký je právní důvod pro zpracování osobních údajů zaměstnance při poskytování benefitů?* [online]. [cit. 2019-04-15]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5057&n=zamestnavatele

správcem zaměstnanců a uchazečů spolu s personální agenturou, která bude pro zaměstnavatele zajišťovat nové zaměstnance a která bude čerpat ze své vlastní databáze uchazečů o zaměstnání (aniž by prováděla specifické oslovování na základě pokynů zaměstnavatele a bylo by ji možné považovat za pouhého zpracovatele).[465] Pokud jde o požadavky nařízení GDPR na takové případy, společní správci by mezi sebou měli transparentním ujednáním vymezit své podíly na odpovědnosti za plnění povinností podle GDPR, zejména pokud jde o výkon práv subjektů údajů a povinnost poskytovat informace o zpracování osobních údajů. Takové ujednání by mělo náležitě zohledňovat úlohy společných správců a jejich vztahy vůči subjektům údajů, přičemž platí, že subjekt by měl být o podstatných prvcích takového ujednání mezi společnými správci informován.[466] Ačkoliv to tedy není výslovně požadováno, s ohledem na požadavek transparentnosti by takové ujednání mělo být v písemné formě a zaměstnavatel a další správce by se o takovém zpracování měli jasně zmiňovat ve svých informačních dokumentech, prostřednictvím kterých je plněna povinnost dle čl. 13 či 14 GDPR.[467]

V případě zaměstnavatelů, u nichž zaměstnanci přicházejí do styku s obchodními partnery či zákazníky zaměstnavatele, bude v úvahu přicházet též určité předávání či spíše jen poskytování určitých údajů zaměstnancům těmto třetím osobám, a to v rámci běžného provozu zaměstnavatele. Může jít též o zpracování osobních údajů zaměstnanců pro potřeby účasti ve veřejné zakázce, kdy je třeba v rámci plnění smluvní zakázek doložit též údaje o dosaženém vzdělání či získaných certifikátech příslušných zaměstnanců. Takové zpracování lze však považovat spíše za náhodné a nesystematické, podle názoru autora této práce by s výjimkou informační povinnosti zaměstnavatele o možnosti takového předávání nemělo být předmětem dalších podmínek.

Závěrem lze poznamenat, že zaměstnavatel by měl, obzvláště u předávání, která nejsou uložena zákonem, za všech okolností posuzovat, zda je takové předávání skutečně nezbytné a zda by stejného cíle nebylo možné dosáhnout i jiným způsobem, kdy by k předávání osobních údajů nedocházelo. Případně by k předávání osobních údajů docházelo, ale pouze v pseudonymizované podobě. Takový postup se nabízí zejména

---

[465] Op. cit. sub. 328.
[466] Viz čl. 26 odst. 1 a 2 GDPR.
[467] Pravděpodobně největší obtíží při zpracování osobních údajů zaměstnanců společnými správci a souvisejícím sdílením osobních údajů bude patrně identifikace toho, že se jedná o vztah společných správců. S ohledem na malé zkušenosti s tímto institutem je v praxi zatím obvykle preferováno nastavení vztahu jakožto dvou samostatných správců, případně vztahu správce-zpracovatel.

u poskytovatelů jednotlivých benefitů (například u stravování), případně u souhlasového předávání obchodním partnerům, kdy může být například pouze kontakt předán zaměstnanci, aby sám obchodního partnera oslovil.

7.6.2 Předávání zpracovatelům

Doposud bylo popisováno pouze předávání osobních údajů třetím osobám, které v návaznosti na předání budou zacházet s předanými osobními údaji zaměstnanců samostatně také jako správci osobních údajů. Kromě toho v praxi běžně dochází k tomu, že zaměstnavatelé využívají též zpracovatelů, kteří osobní údaje zpracovávají pouze výhradně v souladu s pokyny a pro zaměstnavatele. K tomuto bude u zaměstnanců docházet relativně často, neboť zejména střední a menší zaměstnavatelé nemají vlastní personální oddělení, které by bylo pověřeno správou a vedením zaměstnanecké agendy, ale tyto činnosti jsou tzv. outsourcovány na třetí osobu, která tyto služby zaměstnavateli poskytuje na smluvním základě.

Zpracovateli osobních údajů zaměstnanců však nebudou jen tyto společnosti poskytující uvedené služby. Může se jednat dále o společnosti, které budou zaměstnavatelům poskytovat IT služby (od správců systémů po poskytovatele cloudových služeb),[468] poskytovatelé archivačních služeb, společnosti vymáhající pohledávky, poskytovatelé poštovních či kurýrních služeb, fotografové či organizátoři firemních akcí. Za určitých okolností se může jednat také o již zmiňované poskytovatele určitých benefitů zaměstnanců (zejména v situacích, kdy je benefit ve skutečnosti poskytován zaměstnavatelem, který k jeho realizaci pouze využije služeb třetí strany).

Ve vztahu se zpracovatelem je důležité to, že zpracovatel je oprávněn nakládat s údaji pouze v souladu s pokyny správce a pro účely, ke kterým byl příslušným správcem pověřen. Platí přitom, že pro předání osobních údajů zpracovateli a pro zpracování osobních údajů z jeho strany není vyžadován souhlas dotčených subjektů údajů, jelikož je možnost takového předávání obecně umožňována nařízením GDPR. Výměnou za tuto volnost jsou však určité povinnosti stanovené správcům. Předně platí, že o předávání osobních údajů zpracovatelům

---

[468] Poskytovatelé IT služeb by měli být však za zpracovatele považováni pouze v případě, že jejich přístup k osobním údajům zaměstnanců nebude ryze náhodný. Podle názoru ÚOOÚ bude zpracovatelem naopak: *„Provozovatel (části) informačního systému pro správce osobních údajů, externí správce sítě, externí bezpečnostní správce, poskytovatel datového úložiště (cloudu).“* (srov. ÚOOÚ: GDPR (obecné nařízení). *Zpracovatel* [online]. [cit. 2019-04-17]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=33194&n=k-povinnosti-spravcu-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju

k dalšímu zpracování musí správce informovat. V optimálním případě je potřeba konkrétně uvést, jakým konkrétním subjektům mohou být osobní údaje takto předávány. Není-li to možné, je třeba uvést alespoň kategorie zpracovatelů, přičemž v takovém případě by měly podle WP29 být tyto informace *„co nejkonkrétnější, s uvedením druhu příjemce (tj. odkazem na jeho činnosti), oboru, odvětví, pododvětví a místa, kde se příjemce nachází“*.[469]

Ještě důležitější povinností, která je uložena zaměstnavatelům (či obecně správcům) při využívání zpracovatelů, je povinnost uzavřít písemnou smlouvu o zpracování osobních údajů ve smyslu čl. 28 odst. 3 GDPR. Na takové smlouvy je kladeno značné množství požadavků a kromě toho, že ve smlouvě o zpracování osobních údajů musí být stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce, musí zároveň obsahovat celou řadu závazků zpracovatele vymezených v čl. 28 odst. 3 písm. a) až h) GDPR. Aniž by bylo záměrem v této práci rozebírat do detailu jednotlivé náležitosti této smlouvy, lze obecně konstatovat, že správci jsou povinni za všech okolností[470] splnění příslušných závazků po zpracovatelích požadovat a případné nedostatky by byly na jejich úkor. Toto však jen reflektuje skutečnost, že právě správci jsou těmi, kteří jsou v první řadě odpovědni za zpracování osobních údajů a kteří mají určovat, jak takové zpracování bude probíhat, včetně definování podmínek pro zpracovatele.

Dokonce již při samotném výběru zpracovatele by zaměstnavatelé jako správci měli postupovat obezřetně a vybírat *„pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů“*.[471] Toto obvykle nebude nutné u zpracovatelů, se kterými již zaměstnavatelé spolupracují, ale pokud mají být osobní údaje zaměstnanců předány novému obchodnímu partnerovi, měl by být tento partner vždy důsledně prověřen. Ve smyslu dodržení zásady odpovědnosti lze pak také doporučit, aby zaměstnavatelé vedli aktuální přehled všech zpracovatelů (ba dokonce všech příjemců), kterým osobní údaje předávají. A to mimo jiné i s ohledem na již zmiňovanou povinnost informovat subjekty údajů o příjemcích jejich osobních údajů.

---

[469] Srov. WP29: *Pokyny k transparentnosti podle nařízení 2016/679*. (WP 260 rev. 01), vydané dne 29. listopadu 2017, ve znění ze dne 11. dubna 2018, s. 38.

[470] Stranou jsou ponechány specifické situace, kdy lze určité náležitosti či záruky zpracovatelů dokládat schváleným kodexem chování ve smyslu čl. 42 GDPR, resp. kdy by se zpracování řídilo právním předpisy a kdy by nebylo nutné žádnou smlouvu o zpracování osobních údajů uzavírat (srov. čl. 28 odst. 3 a 5 GDPR).

[471] Viz čl. 28 odst. 1 GDPR.

7.6.3 Vybrané další případy předávání

Nad rámec výše uvedeného ještě stojí za analýzu některé specifické případy předávání osobních údajů zaměstnanců, na které lze v praxi narazit. Ve vztahu k osobním údajům zaměstnanců půjde především o sdílení osobních údajů zaměstnanců v rámci koncernů, resp. nadnárodních skupin. Může se ale jednat také o předávní osobních údajů zaměstnanců v rámci akvizic zaměstnavatelů.

Pokud jde o předávání osobních údajů zaměstnanců v rámci skupiny, nelze dělat závěry o zákonnosti takového jednání, aniž budou známy bližší detaily takového předávání. Předně totiž platí, že pro posouzení zákonnosti takového předávání bude nutné nejprve ujasnit účel takového předávání. Obecně nejčastějším důvodem je předávání pro zajištění jednotného skupinového řízení zaměstnanců. Otázkou, která se pak nabízí, je, zda lze takové předávání realizovat výhradně na základě souhlasu zaměstnanců, nebo bez něj s odkazem na jiný právní základ. Odpověď lze částečně nalézt v preambuli GDPR, kde je možné se konkrétně dočíst, že *„správci, kteří jsou součástí skupiny podniků nebo instituce přidružené k ústřednímu orgánu, mohou mít oprávněný zájem na předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely, včetně zpracování osobních údajů zákazníků či zaměstnanců“*.[472] Takové ustanovení by dle názoru autora této práce mělo být čteno tak, že takové předávání uvnitř skupiny bez souhlasu zaměstnance není a priori vyloučeno, je nicméně nutné vždy provést balanční test a v jeho rámci posoudit všechny podmínky a přípustnost takového předávání.[473]

Samostatnou kapitolou poté může být situace, kdy v rámci takového vnitroskupinového sdílení osobních údajů zaměstnanců má docházet k předávání osobních údajů do třetích zemí. V takovém případě bude nutné předně odlišovat, zda se jedná o předávání do jiné země Evropské unie nebo mimo ni. V případě předávání osobních údajů v rámci Evropské unie (resp. v rámci Evropského hospodářského prostoru) je situace relativně jednoduchá, neboť v takové situaci se plně uplatní tzv. zásada volného pohybu osobních údajů, a to mimo jiné díky v podstatě shodné[474] regulaci osobních údajů pro celou Evropskou unii.

---

[472] Viz preambule (48) GDPR.
[473] K balančním testům blíže srov. bod 6.2.3.
[474] Ačkoliv se v rámci celé Evropské unie plně uplatní nařízení GDPR, nelze říci, že by všude byla úprava jednotná, neboť toto nařízení v celé řadě případů umožňuje členským státům přijmout svá odchylná pravidla.

Pokud jde o předávání mimo Evropskou unii, je situace značně komplikovanější. V takovém případě je předávání možné jen v případě splnění dalších podmínek. Jde zejména o předávání založené na rozhodnutí Evropské komise o odpovídající úrovni ochrany osobních údajů ve vybraných zemích,[475] předávání osobních údajů do Spojených států amerických společnostem, které se zavázaly k dodržování zásad programu „Privacy Shield“,[476] předávání založené na vhodných zárukách garantovaných správcem či vývozcem údajů[477] apod. Bližší rozbor uvedených jednotlivých možností přesahuje rozsah této práce, zaměstnavatelé by však měli být při takovémto předávání zvlášť obezřetní. Dostat se do situace, kdy budou předávat osobní údaje zaměstnanců, se přitom mohou snadno nevědomky dostat, zejména při využívání různých cloudových služeb se servery umístěnými mimo hranice Evropské unie.

Jak bylo výše naznačeno, za samostatnou úvahu stojí též možnost předávat osobní údaje zaměstnanců v rámci akvizic (například nákup podílu či akcií ve společnosti) či jiných transakcí. Mnohdy totiž v praxi dochází k tomu, že v rámci právního auditu zájemci vyžadují též informace, které mohou zahrnovat osobní údaje zaměstnanců. Podle názoru autora této práce však takový požadavek obecně nelze akceptovat, zejména pokud jde o identifikační údaje zaměstnanců v souvislosti s jinými údaji, jako je jejich mzda či jiné odměny. Pro zákonnost takového předávání by totiž musel existovat legitimní účel a odpovídající právní základ. Oba tyto prvky však budou obecně chybět. Účelem právního auditu je udělat si relativně bližší představu o stavu a fungování společnosti. Nemusí a nemůže však jít o takovou představu, jakou mají jednatelé společnosti, a to zejména s ohledem na ochranu osobnosti a osobních údajů zaměstnanců, ale také s ohledem na jejich slabší postavení.[478] Pro učinění rozhodnutí bude obecně možné považovat za dostatečné, pokud budou poskytnuty anonymizované údaje (ve smyslu počet zaměstnanců, průměrná mzda apod.).

S tím úzce souvisí neexistence právního základu pro takové předání a zpracování. Jediný právní základ připadající do úvahy by mohl být „oprávněný zájem“ zaměstnavatele

---

[475] Těchto rozhodnutí je celá řada, například rozhodnutí Evropské komise ze dne 26. července 2000 o odpovídající ochraně osobních údajů ve Švýcarsku (2000/518/ES), rozhodnutí Evropské komise ze dne 20. prosince 2001 o odpovídající ochraně osobních údajů v Kanadě (2002/2/ES), rozhodnutí Evropské komise ze dne 30. června 2003 o odpovídající ochraně osobních údajů v Argentině (2003/490/ES) apod.

[476] Rozhodnutí Evropské komise 2016/1250 ze dne 12. července 2016 (C/2016/4176) o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí.

[477] Závazná podniková pravidla (tzv. Binding Corporate Rules) ve smyslu čl. 47 GDPR, standardní smluvní doložky ve smyslu čl. 46 odst. 2 písm. c) GDPR a příslušných rozhodnutí Evropské komise a další.

[478] V konečné řadě také s ohledem na ochranu zájmů zaměstnavatele a citlivost daných informací (vůči případné konkurenci), ač tato skutečnost není relevantní z pohledu předmětu této práce.

či zájemce na takovém předání ve smyslu čl. 6 odst. 1 písm. f) GDPR. V takové situaci by však musel být proveden balanční test a je zřejmé, že by takový balanční test, mimo jiné s ohledem výše zmíněnou na absenci účelu, nemohl vyznít ve prospěch zamýšleného předávání osobních údajů. Pravděpodobně by mohly nastat situace, kdy by s ohledem na specifické skutkové povinnosti bylo takové předávání odůvodněno (a to pokud by došlo k přijetí odpovídajících, resp. zvýšených záruk za bezpečnost a zpracování osobních údajů). Takové případy však budou spíše výjimečné a podle názoru autora této práce lze výše uvedené shrnout tak, že zamýšlené předávání by bylo v rozporu se zásadou zákonnosti zpracování, se zásadou účelového omezení a se zásadou minimalizace zpracovávaných údajů ve smyslu čl. 5 odst. 1 GDPR.

7.7 Záznamy o činnostech, integrita a důvěrnost osobních údajů

Zpracování osobních údajů zaměstnanců vyvolá řadu dalších povinností zaměstnavatelů podle nařízení GDPR. Úplný a detailní rozbor všech povinností přesahuje rozsah této práce, nicméně kromě výše zmíněných povinností, které mají zaměstnavatelé při zpracování osobních údajů zaměstnanců, je ještě několik specifických povinností, u nichž stojí zamyslet se blíže nad rozsahem a podmínkami jejich uplatnění. Důvodem je, že tyto povinnosti jsou významné z hlediska dosažení a prokazování zákonnosti zpracování osobních údajů ze strany zaměstnavatele. Jde především o povinnost vést záznamy o činnostech zpracování, povinnost provádět posouzení vlivu na ochranu osobních údajů, povinnost zajistit odpovídající zabezpečení osobních údajů, případně též povinnost jmenovat pověřence pro ochranu osobních údajů.

7.7.1 Záznamy o činnostech zpracování

Vedení záznamů o činnostech je novinkou, kterou zavedlo nařízení GDPR, a to zejména jako částečnou náhradu za oznamovací povinnost ve smyslu § 16 ZOOÚ.[479] Obsahem této povinnosti je přitom požadavek, aby zaměstnavatel byl schopen doložit soulad zpracování osobních údajů s nařízením GDPR[480] a umožnil dozorovému orgánu udělat si představu o prováděném zpracování osobních údajů, jelikož správce je povinen tyto záznamy vždy předložit na požádání.[481] Na rozdíl od oznamovací povinnosti obsažené v ZOOÚ bude povinnost vedení záznamu širší, neboť ZOOÚ obsahoval výjimku, kdy

[479] Resp. odpovídající povinnost podle čl. 18 Směrnice.
[480] Viz preambule (82) nařízení GDPR.
[481] Srov. ustanovení čl. 30 odst. 4 nařízení GDPR.

nebylo nutné oznámení učinit. Podle § 18 odst. 1 písm. b) se přitom tato výjimka uplatnila na zpracování, které správci ukládá zvláštní zákon. Toto bylo vykládáno tak, že není nutné obecně ohlašovat zpracování osobních údajů zaměstnanců, pokud dochází ke zpracování pouze za účelem vedení personální a mzdové agendy.[482] Záznamy o činnostech zpracování takovou výjimku neobsahují, a zaměstnavatelé jsou proto povinni záznamy vést i ke zpracování prováděným pro tyto účely.

Za zmínku stojí dále skutečnost, že nařízení GDPR nepředpokládá, že by záznamy měly být vedeny za všech okolností. Případy, kdy jejich vedení není nutné, jsou vymezeny v ustanovení čl. 30 odst. 5 GDPR. Jedná se nicméně o natolik úzce vymezenou výjimku, že její uplatnění přijde do úvahy jen v naprostém minimu případů.[483] Podle názoru autora této práce bude vedení záznamů o činnostech vždy nutné, pokud má společnost určité zaměstnance. Pokud jde o obsah záznamů o činnostech zpracování, nařízení GDPR stručně vymezuje, co bude jejich obsahem. S výjimkou některých specifických případů nebylo v tomto ohledu zatím bohužel vydáno ze strany ÚOOÚ žádné stanovisko, které by obsah blíže vymezovalo.[484] Jiný přístup zaujaly zahraniční dozorové orgány, když mnohé již vydaly návod, jak takové záznamy sestavit, včetně vzorů, jak by měly vypadat.[485] Také některé české orgány k řešení této otázky přistoupily a pokusily se správcům metodicky

---

[482] Srov. stanovisko ÚOOÚ č. 6/2012: *Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů*. Březen 2012, poslední revize duben 2013.

[483] To platí zejména s ohledem na část ustanovení čl. 30 odst. 5 GDPR, která uvádí, že záznamy bude nutné vždy vést, pokud zpracování není jen „příležitostné". Pokud má společnost alespoň jednoho zaměstnance, zpracování osobních údajů nebude podle názoru autora této práce nikdy jen příležitostné, ale bude naopak velmi pravidelné a konstantní.

[484] Výjimkou je vzor záznamu o činnostech zpracování pro nejmenší podnikatele, který zveřejnil ÚOOÚ na svých stránkách dne 28. května 2018 (ÚOOÚ: Poradna. *Jaké informace by měl obsahovat záznam o činnostech zpracování pro nejmenší podnikatele?* [online]. [cit. 2019-04-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30185), případně vzor záznamu pro kamerové systémy (ÚOOÚ: Sekce: často kladené dotazy. *Ke kamerám a kamerovým systémům* [online]. [cit. 2019-04-17]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5041&n=ke-kameram-a-kamerovym-systemum)

[485] Výjimkou jsou některé zahraniční dozorové orgány, které jsou v tomto ohledu aktivnější. Jedním z prvních byl v tomto ohledu belgický dozorový orgán, který stihl vydat vzorové záznamy ve francouzštině a holandštině již v roce 2017 (Belgium Data Protection Authority: *Modèle de Registre des activités de traitement.* Published August 2017 [online]. [cit. 2019-04-17]. Dostupné z: https://www.autoriteprotectiondonnees.be/canevas-de-registre-des-activites-de-traitement), případně francouzský dozorový orgán (Commission Nationale de l'Informatique et des Libertés (CNIL): *Le registre des activités de traitement*. [online]. [cit. 2019-04-17]. Dostupné z: https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement). Také britský dozorový orgán vydal podrobný návod, včetně vzoru, jak by záznamy o činnostech zpracování měly být zpracovávány (Information Commissioner's Office (ICO): How do we document our processing activities? [online]. [cit. 2019-04-17] Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/), obdobně též Lichtenštejnský dozorový orgán (Datenschutzstelle Fürstentum Liechtenstein: *Verzeichnis Verarbeitungstätigkeiten (Art. 30 DSGVO)*. [online]. [cit. 2019-04-17]. Dostupné z: https://www.datenschutzstelle.li/datenschutz/themen-z/verzeichnis-verarbeitungstaetigkeiten).

pomoci. Za zmínku stojí zejména vzory vydané ze strany Ministerstva vnitra České republiky, z nichž jeden se týká též přímo vedení personální agendy.[486] Přestože jsou vzory určeny primárně pro obce I. stupně, pokud jde o personální agendu, lze dovozovat též jejich širší využitelnost s ohledem na obecnou platnost podaných informací. Ty totiž nejsou nijak překvapivé a ke stejným závěrům bude nutné dojít ve většině případů zpracování osobních údajů zaměstnanců. Pokud jde o strukturu vzorů, jsou navíc dodrženy požadavky dle čl. 30 odst. 1 GDPR, a proto zejména pro menší zaměstnavatele mohou jistě sloužit jako vhodný zdroj inspirace.

7.7.2 Zabezpečení osobních údajů

Zabezpečení osobních údajů při jejich zpracování nebude mít příliš mnoho specifických odlišností od obecného zpracování osobních údajů jakýchkoliv jiných subjektů. Přesto se jich několik najde. Záměrem tohoto bodu přitom není věnovat se všem povinnostem souvisejícím se zabezpečením osobních údajů, ale jen těm specifikům, které souvisí se zpracováním osobních údajů zaměstnanců.

U zaměstnaneckých osobních údajů bude zvlášť důležité dodržovat povinnost, aby k nim měly přístup jen vybrané osoby a zaměstnanci pověření personální agendou. V případě větších zaměstnavatelů by rozhodně nemělo platit, že každý z nich má přístup ke všemu, ale i mezi nimi je nutná určitá specializace. Toto pravidlo bylo snad u většiny zaměstnavatelů dodržováno ještě před účinností GDPR či dřívějších předpisů upravujících ochranu osobních údajů, a to zejména ve vztahu k informacím týkajícím se mezd a jiných odměn s ohledem na citlivost těchto informací pro zaměstnavatele a s ohledem na snadnou zneužitelnost těchto informací jinými zaměstnanci. Proto dodržování této povinnosti obvykle nebude činit větší obtíže.

V podkapitole 7.4 bylo vysvětleno, že zaměstnavatel může držet též některé zvláštní kategorie osobních údajů. U nich by měli zaměstnavatelé tudíž zajistit zvýšené zabezpečení a možnost pověřených zaměstnanců k nim přistupovat. Jistým specifikem zaměstnavatelů bude také fyzické vedení osobních spisů, v jehož rámci bude obsažena celá řada dokumentů týkajících se zaměstnanců. ZPr sice relativně přesně určuje, kdo může do osobního spisu nahlížet (§ 312 odst. 2 ZPr), jelikož však v konečném důsledku může jít o relativně široký okruh osob či orgánů, měl by zaměstnavatel s ohledem na charakter ve spise obsažených

[486] Ministerstvo vnitra České republiky: *Vzorové dokumenty*. Metodická podpora a konzultace [online]. [cit. 2019-04-17]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/vzorove-dokumenty.aspx?q=cHJuPTE%3d

informací zajistit, aby takové nahlížení bylo vždy řádně odůvodněno, evidováno a omezováno na minimum nezbytných případů. Konečně specifické (zvýšené) nároky na zabezpečení bude ve vztahu ke zpracování osobních údajů zaměstnanců nutné aplikovat rovněž při použití sledovacích či kontrolních mechanismů ve smyslu § 316 ZPr. Získané osobní údaje mohou být s ohledem na využitý monitorovací či sledovací nástroj skutečně velmi choulostivé. To platí zejména ve vztahu využití kamer na pracovišti a využití nástrojů sledujících využití (tj. především počítačů, mobilů apod.).

Zvlášť obezřetně by zaměstnavatelé měli postupovat také v případě, že osobní údaje nebo jejich část uchovávají na úložištích třetích stran, především při využívání tzv. cloudových služeb. Zejména u novějších a menších zaměstnavatelů je využívání takových služeb dnes již obvyklé. V závislosti na možnosti přístupu k osobním údajům lze poskytovatele takových služeb přitom považovat za zpracovatele osobních údajů zaměstnanců, což vyvolává mimo jiné povinnost uzavřít s takovým poskytovatelem smlouvu o zpracování osobních údajů se všemi jejími náležitostmi. Zároveň to ale nezbavuje zaměstnavatele jiných povinností, včetně povinnosti zajistit odpovídající zabezpečení osobních údajů. V tomto ohledu lze souhlasit s názorem ÚOOÚ, že je na zaměstnavateli, aby *„zajistil adekvátní opatření na své straně (např. šifrování dat) a aby si uzavřením smluvních vztahů s případným poskytovatelem služeb cloud computingu ošetřil veškeré podmínky zpracování (zajištění odpovídající úrovně zabezpečení; odpovědnost poskytovatele služeb/zpracovatele za jeho případná selhání s dopady do oblasti ochrany osobních údajů, garantování nevratné likvidace údajů apod.)“*.[487] Platí tedy, že nejen neoprávněné užití osobních údajů zaměstnanců může mít nedozírné následky, ale obdobně též jejich ztráta. Jak bylo uvedeno výše, zaměstnavatel má celou řadu zákonných povinností týkajících se uchování osobních údajů zaměstnanců. Zejména z hlediska sociálního zabezpečení by ztráta takových osobních údajů mohla mít závažné negativní dopady na zaměstnance.

Specifické otázky týkající se zabezpečení mohou nastat také v případě osobních údajů uchazečů o zaměstnání. Nikoliv výjimečně u zaměstnavatelů dochází k tomu, že životopis uchazeče s nejrůznějšími jeho osobními údaji putuje nejen k příslušným osobám majícím na starosti výběrové řízení, ale též k osobám, které se na výběrovém řízení jen

[487] ÚOOÚ: Sekce: často kladené dotazy. *Zaměstnavatelé, Jaké jsou základní podmínky pro zpracování firemních i zaměstnaneckých dat v tzv. „cloudu“?* [online]. [cit. 2019-04-17]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5057&n=zamestnavatele

podílejí, nebo dokonce ani žádnou působnost v tomto ohledu nemají. To je způsobeno zejména tím, jak snadné je přeposílání e-mailů s přílohami. Z hlediska uchazečů o zaměstnání a nakládání s jejich osobními údaji je taková situace zcela nevyhovující, nemluvě o skutečnosti, že v takovém případě je v podstatě nemožné zajistit likvidaci osobních údajů uchazeče po uplynutí doby k jejich zpracování, neboť zaměstnavatel má mizivou kontrolu nad takovými osobními údaji. Těmto excesům se lze přitom relativně jednoduše bránit tím, že budou interně jasně nastavena a kontrolována pravidla a odpovědnost za zacházení s takovými údaji.

7.7.3 Posouzení vlivu na ochranu osobních údajů

Jednou z nových povinností, kterou zavedlo nařízení GDPR je též provádět tzv. posouzení vlivu na ochranu osobních údajů ve smyslu čl. 25 GDPR. Jedná se o nástroj, jehož účelem je provést před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů, a to v případech, kdy bude pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob.[488]

Situace, ve kterých bude nutné posouzení vlivu provádět, jsou demonstrativně vymezeny v čl. 35 odst. 3 GDPR. Některé indicie, kdy bude nutné posouzení vlivu zpracovat, lze rovněž dovodit z preambule nařízení GDPR. Komplexní shrnutí lze pak nalézt v příslušném stanovisku WP29.[489] Záměrem tohoto bodu nicméně není blíže zkoumat jednotlivé případy, kdy bude nutné zpracování provádět, ale zamyslet se nad tím, zda některé takové případy budou relevantní při zpracování osobních údajů zaměstnanců.

WP29 vychází při určení, kdy bude nutné zpracovávat posouzení vlivu, z devíti různých kritérií, přičemž pro vznik povinnosti vypracovat posouzení vlivu stačí, aby při zpracování nastala alespoň dvě z těchto devíti kritérií.[490] Při zpracování osobních údajů zaměstnanců bude relevantní zejména kritérium č. 7, které uvádí, že bude docházet ke zpracování údajů zranitelných subjektů. Za ty jsou totiž považováni mimo jiné zaměstnanci. Při výkladu WP29 by pak splnění v podstatě jakéhokoliv dalšího kritéria mělo vést

[488] Srov. ustanovení čl. 35 odst. 1 GDPR.
[489] WP29: Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679. (WP 248 rev. 01), vydané dne 4. dubna 2017, ve znění ze dne 4. října 2017.
[490] Op. cit. sub. 489, s. 10 až 12.

k povinnosti posouzení vlivu zpracovat. Nabízí se především kritérium č. 5, předpokládající zpracování ve velkém měřítku (pro větší zaměstnavatele), kritérium č. 3, předpokládající systematické monitorování, kritérium č. 1, týkající se hodnocení nebo bodování, které může souviset též s hodnocením pracovního výkonu, nebo dokonce kritérium č. 4, týkající se zpracování citlivých údajů či údajů vysoce osobní povahy. Podle výkladu WP29 se tak bude jednat o rozsáhlý počet případů, kdy by zaměstnavatelé měli být povinni posouzení vlivu zpracovávat.

ÚOOÚ zveřejnil k této otázce vlastní metodologii, která částečně z pokynů WP29 vychází, částečně je ale přepracovává.[491] ÚOOÚ přináší seznam celkem 10 druhů operací zpracování (či 10 kritérií), ke kterým definuje škálu rizikovosti, resp. tři intervaly hodnot, kterých mohou nabývat, a to od kritické hodnoty přes významnou hodnotu až po nízkou hodnotu rizikovosti. Pro povinnost vyhotovit posouzení vlivu se přitom vyžaduje, aby zpracování dosahovalo alespoň dvakrát kritické hodnoty, nebo jedenkrát kritické hodnoty a alespoň pětkrát významné hodnoty.[492] Jelikož jde už o relativně složitý systém, není prostor jej zde blíže popisovat. Důležité však je, že při aplikaci těchto pravidel na zpracování osobních údajů zaměstnanců bude nutné dojít k relativně odlišným závěrům od závěrů vyplývajících z pokynů WP29, a to právě s ohledem na rozpracování stupňů rizikovosti.

Předně jakýkoliv monitoring zaměstnanců je považován za kritický. Aby bylo nutné zpracovávat posouzení vlivu, je však nezbytné, aby bylo naplněno ještě další kritérium. Tím obecně není podřízení či zranitelnost zaměstnanců, neboť tento aspekt je na stupnici rizikovosti považován „pouze“ za významnou hodnotu. Pokud jde o rozsah zpracování, muselo by docházet ke zpracování osobních údajů alespoň 10 tisíc subjektů údajů. Pokud by dotčených subjektů bylo v rozmezí od 5 tisíc do 10 tisíc, šlo by rovněž „jen“ o významnou hodnotu. Tento aspekt tedy bude důležitý jen u skutečně velkých zaměstnavatelů. Z hlediska nutnosti posouzení vlivu zaměstnanců pak mohou být dále významná zejména kritéria zpracování „kritických“ údajů (nejen zvláštní kategorie osobních údajů ve smyslu čl. 9 GDPR, ale též údaje vysoce osobní povahy, jako je historie navštívených stránek či údaje elektronické pošty; jde o kritickou hodnotu) či zavedení zcela nových nebo inovativních řešení (rovněž jde o kritickou hodnotu).[493]

---

[491] ÚOOÚ: GDPR (obecné nařízení). *K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů*. Publikováno dne 8. února 2019 [online]. [cit. 2019-04-21]. Dostupné z: https://www.uoou.cz/k-povinnosti-spravcu-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/ds-5458/archiv=0&p1=3938

[492] Op. cit. sub. 491, s. 3.

[493] Op. cit. sub. 491, s. 4 až 11.

S ohledem na výše uvedené je zřejmé, že okruh činností, kdy bude nutné posouzení vlivu zpracovat podle metodiky ÚOOÚ, je značně užší. V zásadě půjde vždy o případy využívání monitorovacích systémů.[494] U dalších případů zpracování už však bude nutné hledat nějaký další specifický aspekt, jako může být velikost zaměstnavatele, využití nové technologie či zpracování kritických údajů. Tím je okruh případů, kdy bude nutné zpracovat posouzení vlivu oproti pokynům WP29, značně zúžen. Tento přístup ÚOOÚ lze podle názoru autora této práce hodnotit velmi kladně a přiléhavě, neboť jiný výklad by neúměrně zatěžoval zaměstnavatele, kteří by při i relativně obvyklých činnostech byli nuceni posouzení vlivu zpracovávat.

7.7.4 Pověřenec pro ochranu osobních údajů

Při analýze požadavků zpracování osobních údajů by bylo chybou nevěnovat pozornost rovněž novému institutu, kterým je nutnost za určitých okolností dle čl. 37 GDPR jmenovat pověřence pro ochranu osobních údajů. Opět není záměrem do detailu analyzovat tento institut z obecného hlediska, například kdy jsou a kdy nejsou dány podmínky pro jmenování pověřence, jaké jsou požadavky na jeho kvalifikaci či jaké jsou jeho úkoly,[495] ale spíše se zaměřit na jeho postavení v případě, že jde o zaměstnance, a na význam ve vztahu ke zpracování osobních údajů zaměstnanců.

Není pochyb o tom, že pověřenec může být též zaměstnancem společnosti (zaměstnavatele).[496] Takové jeho postavení však může vyvolávat řadu otázek, zejména z hlediska pracovního práva, neboť zaměstnavatel musí zajistit, aby pověřenec nedostával žádné pokyny týkající se výkonu jeho úkolů dle čl. 39 GDPR, v souvislosti s plněním svých úkolů nemůže zaměstnavatel pověřence propustit ani sankcionovat a musí zajistit, aby byl přímo podřízen vrcholovým řídícím pracovníkům zaměstnavatele.[497] Bylo by skutečně neplatné rozvázání pracovního poměru, pokud by výpověď splňovala požadavky ZPr, ale odporovala by ustanovením GDPR? Jaká je tedy odpovědnost pověřence za chybné plnění jemu svěřených úkolů a je limitována shodně jako obecná odpovědnost zaměstnanců ve smyslu § 257 a násl. ZPr? Podle názoru autora této práce je nutné na tyto otázky odpovědět

[494] V tomto případě bude splněno kritérium monitoringu a kritických údajů či inovativních řešení.
[495] K tomu blíže srov, WP29: Pokyny týkající se pověřenců pro ochranu osobních údajů. (WP 243 rev. 01), vydané dne 13. prosince 2016, ve znění ze dne 5. dubna 2017.
[496] Čl. 37 odst. 6 GDPR.
[497] Čl. 38 odst. 3 GDPR.

kladně a ochranu pro takového zaměstnance dovozovat.[498] Obdobně pak může činit obtíže povinnost zajistit, aby v případě pověřence nedocházelo ke střetu zájmů (toto bude obvykle hrozit u vedoucích pracovníků, jako jsou ředitelé, jednatelé, vedoucí HR, vedoucí IT apod.).[499] V souvislosti s nutností zajistit, aby byl pověřenec při plnění svých úkolů podřízen přímo vedení společnosti, pak může být ve schizofrenní roli vůči svým nadřízeným.

Výše popsané problémy jsou však záležitosti, které se naprosté většiny běžných zaměstnanců nijak nedotknou. Z jejich hlediska bude významné, že v případě jmenování pověřence pro ochranu osobních údajů bude v jejich společnosti působit vždy někdo, na koho se mohou snadno obracet se svými problémy a obavami týkajícími se ochrany jejich soukromí a zpracování jejich osobních údajů.[500] Podle názoru autora této práce je přitom nutné dovozovat působnost pověřenců též plně ve vztahu ke zpracování osobních údajů zaměstnanců a specifikům vyjádřeným v rámci ZPr, zejména pokud jde o požadavky jeho § 316. Na pověřencích především bude, aby zaměstnavatele upozornili na zákonem stanovené mantinely při využívání různých monitorovacích systémů (a nejen jich) a upozornili zaměstnavatele na povinnost zachovávat ochranu soukromí zaměstnanců, neboť ta je s ochranou osobních údajů neoddělitelně spjata. Z tohoto hlediska lze institut pověřenců pro ochranu osobních údajů jednoznačně přivítat, a to i přesto, že povinnost jeho jmenování přináší pro zaměstnavatele dodatečné náklady.

---

[498] Je ovšem nutné tyto záležitosti posuzovat ad hoc s ohledem na skutkové okolnosti, neboť i plnění úkolů svěřených GDPR může být zanedbáváno natolik, že může vést k rozvázání pracovního poměru, případně též zvláštní smlouvy, na základě které pověřenec svou funkci vykonává. Ochrana dle čl. 38 odst. 3 GDPR má být podle názoru autora této práce vykládána tak, aby pověřence ochraňovala před jeho výhradami k postupům zaměstnavatele při zpracování osobních údajů. K obdobným závěrům dochází též Nulíček (Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 345).

[499] Op. cit. sub. 495, s. 27.

[500] Neplatí automaticky, že v případě zaměstnavatelů, kde žádný pověřenec jmenován nebude, by tato možnost neměla existovat, nicméně tam, kde pověřenec bude, to bude pro zaměstnance obvykle jednodušší.

IV. ČÁST VYBRANÉ APLIKAČNÍ OTÁZKY A SHRNUTÍ

8 Vybrané praktické aspekty ochrany zaměstnanců

Záměrem této kapitoly je blíže analyzovat vybrané a nejčastěji využívané nástroje pro monitorování zaměstnanců ze strany zaměstnavatelů a podrobit je kritickému hodnocení z hlediska úpravy ochrany osobnosti zaměstnanců i z hlediska právní úpravy na ochranu osobních údajů. Spolu s tím bude též zhodnocena relevantní judikatura. Kromě tématu monitoringu zaměstnanců se tato kapitola věnuje rovněž dvěma dalším vybraným otázkám, kterými jsou stále více a více se rozšiřující whistleblowing a screening neboli odhalování majetku zaměstnanců ze strany jejich zaměstnavatelů.

8.1 Monitoring zaměstnanců v praxi

Jak již bylo popsáno, zaměstnavatelé ve snaze chránit svůj majetek a dohlížet na výkonnost svých zaměstnanců používají nejrůznější monitorovací a sledovací prostředky, mechanismy či postupy. Rozvoj informačních technologií v posledních desetiletích přinesl z tohoto hlediska zaměstnavatelům řadu nástrojů, jak těchto cílů dosahovat. A ačkoliv není vyloučeno, že do budoucna nebudou do praxe zavedeny další nové nástroje, lze charakterizovat a kriticky zhodnotit ty nejčastěji dnes využívané. Jedná se především o sledování písemností zaměstnanců, sledování elektronické pošty, využívání informačních technologií, včetně prohlížení webových stránek, sledování pomocí kamer či GPS technologií.

Záměrem následujících bodů je tyto fenomény kriticky rozebrat a zhodnotit z hlediska nutnosti aplikace pravidel, o kterých byl podán výklad v předchozích kapitolách. Půjde tedy nejen o aplikaci ochranných ustanovení v rámci ZPr, ale též o aplikace norem na ochranu osobních údajů. Je totiž nezpochybnitelné, že při využívání těchto nástrojů pro kontrolu a sledování zaměstnanců bude vždy docházet též ke zpracování jejich osobních údajů, a to mnohdy velmi citlivých.

8.1.1 Písemnosti zaměstnanců (kontrola listovních zásilek)

Problematika ochrany písemností je dnes spíše na okraji. Relevantní byla spíše v minulosti, kdy informační technologie ještě nebyly tolik rozšířené, resp. kdy vůbec neexistovaly. Přesto má tato ochrana význam i dnes, a proto bude alespoň v krátkosti

zkoumána i zde. Jde o problematiku toho, kdy může zaměstnavatel do soukromých písemností, které si zaměstnanci zřejmě vyřizují během pracovní doby, nahlížet, číst je, dovozovat z nich důsledky, případně je zaměstnancům zakazovat.[501]

Při hledání odpovědi na otázku, kdy může a kdy nemůže zaměstnavatel kontrolou těchto písemností narušovat soukromí, jde o tradiční problém dvou ústavním pořádkem (dle LZPAS) chráněných práv. Na jedné straně stojí právo na ochranu soukromí a listovního tajemství dle čl. 10 a 13 LZPAS, na druhé straně stojí ochrana majetku zaměstnavatele dle čl. 11 LZPAS. Zde je nicméně ochrana zaměstnanců navíc dále posílena zvláštními pravidly dle § 316 odst. 2 ZPr, která omezují možnost zaměstnavatele zasahovat do soukromí zaměstnanců na skutečně výjimečné případy. Proto zaměstnavatel obecně nebude mít právo do listovních zásilek zasahovat. V tomto případě nemůže ani argumentovat tím, že by prováděl kontrolu svěřených výrobních a pracovních prostředků ve smyslu § 316 odst. 1 ZPr, neboť to z podstaty věci nepřipadá do úvahy, resp. je zanedbatelné. A pokud by už u zaměstnavatele nastal závažný důvod spočívající ve zvláštní povaze činnosti ve smyslu § 316 odst. 2 ZPr, i tak by měl zaměstnavatel limitovat jakékoliv zasahování do obsahu listovních zásilek na nezbytné minimum případů, které by pro definované účely bylo dostatečné.

Určitou komplikací může být způsob, jak zaměstnavatel odliší písemnosti soukromé od písemností pracovních či služebních, na které se tato ochrana nevztahuje. ÚOOÚ se v tomto ohledu snaží být nápomocný svým výkladem, když vyjadřuje, že předně lze písemnost odlišovat podle obálky. U soukromé obálky je jméno a příjmení uvedeno na prvním místě a název zaměstnavatele slouží pouze jako adresní údaj. U pracovních zásilek je tomu naopak.[502] Pokud je na obálce uvedeno „k rukám [jméno osoby]“, jde už o spornou věc, spíše by se však mělo jednat pracovní zásilku.[503] Ačkoliv tento výklad jistě nebude možné použít ve všech případech, v mnoha případech z něj bude možné alespoň vycházet do té doby, než se prokáže opak.

Z hlediska ochrany osobních údajů je nepochybné, že obsah těchto soukromých zásilek bude možné považovat za osobní údaje zaměstnance (a obvykle též třetích osob). Výše však bylo vysvětleno, že zaměstnavatel by se k těmto údajům v podstatě nikdy neměl

[501] S nadsázkou lze toto přirovnat k psaníčkům dětí ve školách.
[502] Stanovisko ÚOOÚ č. 2/2009: *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*. Únor 2009. (Při tomto výkladu se ÚOOÚ odvolává na rozhodnutí Českého telekomunikačního úřadu.)
[503] Tamtéž.

dostávat. Pokud nastane některý z případů podle § 316 odst. 2 ZPr, bude právním základem pro zpracování obvykle oprávněný zájem zaměstnavatele ve smyslu čl. 6 odst. 1 písm. f) GDPR (kdy bude nutné též zpracovat balanční test).[504] Samozřejmostí bude povinnost o tomto sledování zásilek a zpracování osobních údajů informovat, a to jak dle § 316 odst. 3 ZPR, tak i dle čl. 13 GDPR.

8.1.2 Elektronická komunikace – e-maily

Oproti ochraně listovních zásilek je v dnešní době mnohem častěji diskutována ochrana elektronické komunikace prostřednictvím e-mailů, případně prostřednictvím jiných elektronických komunikačních služeb a nástrojů.[505] Je to díky současnému rozšíření informačních technologií. V případě těchto komunikačních prostředků budou základní východiska shodná jako v případě písemností či listovních zásilek. I v tomto případě proti sobě stojí ochrana soukromí a listovního tajemství zaměstnance a ochrana majetku zaměstnavatele. I v tomto případě má důležitý význam ustanovení § 316 odst. 2 ZPr, které umožňuje v určitých případech elektronickou komunikaci sledovat, ale i tak je třeba dodržovat LZPAS chráněné listovní tajemství. Obdobného názoru je, resp. byla též WP29, která se vyjádřila takto: *„Na obsah elektronické komunikace posílané z pracovních prostor se vztahují stejná základní práva ochrany jako na komunikace analogové.“*[506]

Přece však bude možné určité specifikum v případě elektronické komunikace oproti písemné komunikaci nalézt, a to je aplikace ustanovení § 316 odst. 1 ZPr. V případě elektronické komunikace zaměstnanců, kterou je zaměstnavatel schopen sledovat, jsou obvykle využívané svěřené pracovní prostředky. Nemusí jít nutně o hardware, stačí softwarové vybavení, licence, účet zaměstnavatele apod. To proto povede k možnosti zaměstnavatele zakázat využívání takových prostředků pro osobní potřebu ve smyslu tohoto ustanovení a možnosti zaměstnavatele tento zákaz přiměřeným způsobem kontrolovat. Při výkladu toho, co lze považovat za přiměřený způsob kontroly, se dá odkázat na stanovisko ÚOOÚ, které uvádí, že je možné *„pouze sledovat počet došlých a odeslaných e-mailů,*

---

[504] Přínosem balančního testu v tomto případě nebude ani toliko rozhodnutí o zpracování, ale především zhodnocení rizik zpracování a zavedení odpovídajících záruk organizačního a technického zabezpečení osobních údajů.

[505] Dále popisovaná pravidla a závěry se uplatní rovnocenně na jakékoliv jiné obdobné komunikační nástroje (Whatsapp, Facebook Messenger, Viber apod.), jakož i na jakékoliv elektronické dokumenty (*.doc, *.xls, *.pdf apod.), má-li jejich obsah soukromý charakter. Obdobně je lze aplikovat dále též na obsah telefonické komunikace.

[506] Stanovisko WP29 č. 2/2017: Zpracování údajů na pracovišti (v originále: *opinion 2/2017 on data processing at work)*. (WP249), ze dne 8. června 2017, s. 3.

případně (tj. zejména vznikne-li podezření ze zneužití pracovních prostředků, resp. využití k jiným než pracovním účelům) včetně hlavičky, tj. komu píší a od koho je dostávají".[507] Na základě těchto dat totiž bude zaměstnavatel obvykle schopen usuzovat na charakter takové komunikace (zda se týká práce či jde o soukromou komunikaci). Zaměstnavatel by tedy neměl být oprávněn číst elektronickou komunikaci svých zaměstnanců.[508] Budou-li však dány podmínky pro postup dle § 316 odst. 2 ZPr, budou oprávnění zaměstnavatele obecně širší a v takovém případě bude též přijatelné, aby zaměstnavatel sledoval též obsah takové komunikace. I tak by opět mělo platit, že zaměstnavatel by se této činnosti měl zdržet tam, kde takovýto postup není nutný.[509]

Nutnou podmínkou pro zákonnost jakýchkoliv kontrol či sledování elektronické komunikace zaměstnanců je splnění informační povinnosti. I kdyby u zaměstnavatele nebyl dán důvod pro sledování dle § 316 odst. 2 ZPr a nebylo by tudíž nutné aplikovat informační povinnost dle § 316 odst. 3 ZPr, bude se při jakékoliv kontrole jednat samozřejmě též o zpracování osobních údajů (byť se bude jednat jen o hlavičky e-mailů a příjemce). Z hlediska zpracování osobních údajů a monitorování elektronické komunikace je významný dokument WP29 týkající se sledování elektronických komunikací na pracovišti.[510] Přestože s ohledem na specifika naší regulace a běžné fungování pracovního prostředí nejsou všechna doporučení použitelná (například aby zaměstnavatelé vytvářeli zaměstnancům dva e-mailové účty – jeden pracovní, který budou monitorovat, a druhý soukromý),[511] v mnoha jiných doporučeních se lze inspirovat pro zavedení dobré praxe.

---

[507] Stanovisko ÚOOÚ č. 2/2009: *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*. Únor 2009. Úřad pro ochranu osobních údajů k tomu dále uvádí: *„Soukromý e-mail zaměstnance smí zaměstnavatel na základě oprávnění daných mu novým zákoníkem práce otevřít a přečíst pouze výjimečně, v zájmu ochrany svých práv […] a jestliže je pravděpodobné, že […] by k jejímu vyřízení zaměstnancem mohlo dojít natolik pozdě, že by zaměstnavatel mohl utrpět újmu na svých právech. Zaměstnavatel tak fakticky využívá svého práva chránit majetek podle nového zákoníku práce."* S těmito závěry se lze v zásadě ztotožnit.

[508] Ke stejnému závěru dochází též Štědroň (viz Štědroň, B. *Čtení e-mailové pošty zaměstnavatelem a ochrana soukromí*. Bulletin advokacie. 2004. č. 10, s. 50).

[509] Zde lze odkázat na výklad podaný v preambuli (24) směrnice 2002/58/ES ze dne 12. července 2002 o soukromí a elektronických komunikacích, ve které se uvádí: *„Koncové zařízení uživatelů sítí elektronických komunikací a jakékoli informace uchovávané na takovém zařízení tvoří součást soukromí uživatelů, které vyžaduje ochranu v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod. Tzv. špionážní software („spyware"), webové štěnice („web bugs"), skryté identifikátory a jiné podobné nástroje mohou pronikat do koncového zařízení uživatele bez jeho vědomí s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost uživatele a mohou vážně narušit soukromí těchto uživatelů […]."*

[510] Pracovní dokument WP29: Ke sledování elektronických komunikací na pracovišti (v originále: *Working document on the surveillance of electronic communications in the workplace*). (WP55), ze dne 29. května 2002. Byť jde již o starší dokument, WP29 se na závěry v něm obsažené odkázala i v roce 2017, v rámci stanoviska WP249.

[511] Tamtéž, s. 5.

Právním základem pro zpracování těchto osobních údajů bude ve většině případů oprávněný zájem zaměstnavatele, což povede k nutnosti provést balanční test. Zaměstnavatel tak bude muset dodržovat mnoho základních principů, aby takové zpracování osobních údajů bylo zákonné. Bude jej muset omezit na nezbytné případy, bude muset jasně definovat účel zpracování, bude muset zpracovávat je přiměřený rozsah osobních údajů (např. jen hlavičky e-mailů, pokud to bude dostatečné), bude muset řádně zaměstnance informovat, bude muset shromážděná data dostatečně zabezpečit a bude muset prokázat, že ochrana jeho práva převažuje nad ochranou soukromí zaměstnanců.

Pokud jde o možnost zasahovat do obsahu, uzavírá WP29 jasně, že na elektronickou komunikaci vykonanou na pracovišti je třeba plně aplikovat koncept „soukromého života" ve smyslu čl. 8 odst. 1 EÚLP, přičemž se odkazuje na již v této práci citované rozhodnutí ve věci Halford vs. Spojené království. Určitou otázkou však zůstává, kde jsou hranice pro možnost omezení tohoto práva. V případě České republiky je podle názoru autora této práce nutné tyto hranice hledat především ve výkladu již zmíněného § 316 ZPr a ochranou listovního tajemství zaměstnanců, resp. ochranou majetku zaměstnavatele. Lze navíc souhlasit se závěry WP29, že při vyvažování těchto práv je namístě vycházet z balančního testu, který je právě tak nutným předpokladem pro zpracování s odkazem na oprávněný zájem zaměstnavatele.

WP29 se dokonce zaobírá možností sledování soukromých schránek zaměstnance (např. přistupovaných skrze webové rozhraní v pracovní době) a uzavírá, že jejich sledování je možné opravdu jen ve výjimečných případech, jako je podezření na kriminální činnost zaměstnance.[512] Podle názoru autora této práce je však otázkou, zda by v takovém případě neměla dané skutečnosti spíše prověřovat policie namísto zaměstnavatele, který by na ně měl pouze upozornit. Kromě toho lze však v zásadě souhlasit se závěrem, že používání takovýchto schránek by mělo být zaměstnavateli v zásadě umožněno. Ve většině případů to odstraní problém s rozlišováním soukromé a pracovní pošty v poštovní schránce zaměstnance zřízené zaměstnavatelem, neboť veškeré e-maily v této schránce budou považovány za pracovní a využívání pracovní doby k řešení soukromých záležitostí bude moci zaměstnavatel kontrolovat dle času stráveného zaměstnancem na příslušné soukromé schránce (aniž by musel sledovat její obsah).[513]

[512] Tamtéž, s. 21.
[513] Tamtéž, s. 23.

Pokud jde o soudní rozhodnutí, která by se této problematice věnovala, není jich příliš. Na české scéně neexistuje prakticky žádné relevantní.[514] Pravděpodobně nejvýznamnějším bude již citované rozhodnutí Velkého senátu ESLP ze dne 5. září 2017 ve věci Barbulescu vs. Rumunsko, č. stížnosti 61496/08. Blíže bylo toto rozhodnutí již rozebíráno v podkapitole 3.4 v souvislosti s výkladem o legitimním očekávání soukromí zaměstnanců na pracovišti, a proto není nutné toto rozhodnutí opět blíže zkoumat. Ačkoliv zaměstnanec byl v tomto případě úspěšný a domohl se odškodnění za nepřiměřený zásah do svého soukromí, když zaměstnavatel sledoval obsah jeho komunikace, aniž by to bylo nezbytné, lze v tomto rozhodnutí spatřovat určitou skepsi. Svého práva se zaměstnanec domohl u ESLP až před Velkým senátem ESLP jakožto posledním možném opravném prostředku po usilovném boji a jeho odškodnění bylo relativně zanedbatelné. Na škodu rovněž je, že soudy v daném řízení blíže neshledaly, ačkoliv toto také bylo zkoumáno, závažnější porušení pravidel na ochranu osobních údajů. Pozitivum však lze vidět v tom, že bylo definováno, jak by na tento a obdobné případy mělo být nahlíženo a jaká pravidla a skutečnosti by měly být hodnoceny, tj. předchozí informování zaměstnance o možnosti a podmínkách kontrol, rozsah přípustného sledování a míra zásahu do soukromí (obsah komunikace vs. obecné informace), skutečný či oprávněný důvod zaměstnavatele pro výkon kontrol či sledování, principy subsidiarity a proporcionality, následky pro zaměstnance. Ve větší míře tedy odpovídají nárokům na provádění balančních testů.

8.1.3 Využití informačních technologií, prohlížení webu

Dalším z kontrolních a monitorovacích nástrojů, který zaměstnavatelé stále hojněji využívají, jsou různé mechanismy umožňující sledování, jakým způsobem zaměstnanci využívají svěřené informačních technologie (zejména osobní počítače, notebooky, tablety, mobily apod.), včetně dohledu nad konkrétními jednáními zaměstnance od psaní dokumentů, využívání aplikací až po prohlížení webu apod. Takovéto nástroje například umožňují jedna ku jedné zobrazovat práci zaměstnance na jiném zařízení nebo jen monitorovat některé prvky této práce. V případě, že by některá taková jednání zaměstnance bylo možno považovat za korespondenci či komunikaci, uplatnily by se plně závěry vyjádřené v předchozím bodě 8.1.2. To však není záměrem v tomto bodě zkoumat. Cílem

[514] Případ Kasalova Pila (tj. rozhodnutí Nejvyššího soudu ČR ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011) se netýká přímo elektronické komunikace, ale spíše využívání PC a prohlížení webů, které je rozebráno v dalším bodě.

v tomto bodě je naopak zaměřit se na ostatní formy využití informačních technologií, kdy obecně není možné dovozovat ochranu listovního tajemství, ale zaměstnanci bude svědčit „pouze“ ochrana jeho soukromí.

Nemožnost aplikace ochrany listovního tajemství bude tedy hlavním rozlišujícím prvkem pro závěry podané v tomto bodě. To však rozhodně neznamená, že by zaměstnanci nebyli chráněni. I nadále se plně uplatní ochrana soukromí zaměstnance či pravidla dle § 316 odst. 1 a 2 ZPr. Pro oprávněnost zásahu do soukromí tak bude nutné hledat dovolenou míru zásahu do soukromí. V případě sledování již zmiňovaných elektronických komunikačních prostředků bude vždy velmi limitovaná, neboť ochrana soukromí je umocněna právě ochranou listovního tajemství. Nebude-li se jednat o elektronickou komunikaci, bude nutné tuto míru vždy ad hoc posuzovat s ohledem na konkrétní opatření prováděné či využívané zaměstnavatelem. Jiná míra ochrany bude v případě sledování technických logů zaměstnance, jiná bude v případě sledování jednání zaměstnance, kdy je jeho činnost jedna ku jedné v reálném čase zrcadlena na jiném zařízení.

Bude tedy nutné vždy vycházet z principů subsidiarity a proporcionality. To zdůrazňuje též ÚOOÚ,[515] který odkazuje na preambuli (26) Směrnice o soukromí a elektronických komunikacích, ve které se mimo jiné uvádí, že údaje o účastnících, které jsou zpracovávány v rámci sítí elektronických komunikací, obsahují informace o soukromém životě fyzických osob.[516] ÚOOÚ sice dále uvádí, že sledování využívání webových stránek obecně není možné, nejsou-li u zaměstnavatele dány závažné důvody spočívající ve zvláštní povaze činnosti zaměstnavatele (§316 odst. 2 ZPr). V takovém případě by obecně (staticky) nemělo docházet ke sledování doby strávené zaměstnancem na internetu,[517] ale zároveň je zaměstnavatel oprávněn zaměstnance postihnout, pokud nevyužívá řádně pracovní dobu a svěřené prostředky.[518] Ač jsou tyto závěry ÚOOÚ částečně nejednoznačné, lze podle výkladu autora této práce dojít k závěru, že k monitoringu využívání informačních technologií mohou zaměstnavatelé přistoupit v zásadě za stejných podmínek, jako je tomu u sledování elektronické komunikace popsané v předchozím bodě. Na rozdíl od sledování elektronické komunikace si však v tomto případě lze dle názoru

[515] Stanovisko ÚOOÚ č. 2/2009: *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*. Únor 2009.
[516] Preambule (26) směrnice Evropského parlamentu a Rady2002/58/ES o soukromí a elektronických komunikacích.
[517] S tímto se autor této práce doslovně neztotožňuje. Ze stanoviska však není zřejmý názor ÚOOÚ na tuto problematiku.
[518] Op. cit. sub. 515.

autora této práce představit širší spektrum kontrolních mechanismů, které by zaměstnavatel mohl využívat jako přiměřený způsob kontroly ve smyslu § 316 odst. 1 ZPr (u elektronické komunikace se takové kontroly mohly omezit v podstatě jen na hlavičku, příjemce a související popisné informace o doručovaných zprávách).

Podíváme-li se do zahraničí, resp. na názory WP29, je relevantní posouzení nabídnuto v již zmiňovaném stanovisku týkajícím se sledování elektronických komunikací na pracovišti.[519] V tomto stanovisku je dovozováno, že zaměstnavatelé by měli možnost využívání či spíše zneužívání těchto svěřených pracovních prostředků sami technickými prostředky regulovat a tím předcházet potenciálně konfliktním situacím. Zároveň se však dodává, že taková regulace by nikdy neměla spočívat v úplném zákazu či znemožnění takového využití. Spíše by mělo jít o omezení rozsahu (zákaz přístupu na některé weby) a doby (zákaz v určitou část pracovní doby). V návaznosti na to jsou definovány základní principy, kterými by mělo být, že (i) prevence by měla být více preferovaným nástrojem oproti detekci a sledování, (ii) zaměstnavatel by měl okamžitě zaměstnance na prohřešek upozornit a nekumulovat proti němu důkazy, nesledovat obsah, (iii) při hodnocení těchto prohřešků by měl zaměstnavatel postupovat mírně, neboť navštívení mnohých webů může být mnohdy neúmyslné (zaviněné přesměrováním webových stránek, bannery apod.) a (iv) zaměstnavatel by měl o těchto nástrojích jasně informovat v rámci svých interních předpisů (a to nejen obecně, ale i s detaily o takovém monitorování).[520]

Zajímavým pramenem je v této souvislosti též Code of Practice vydaný ze strany Mezinárodní organizace práce, v jehož rámci je rozebíráno, za jakých podmínek by mělo být připuštěno skryté sledování. To by mělo být možné, pokud to bude v souladu s národní legislativou nebo pokud bude mít zaměstnavatel důvodné podezření na trestnou činnost či jiný závažný prohřešek zaměstnance.[521]

Pokud jde o soudní rozhodnutí, není v tomto případě nutné hledat v zahraničních vodách, ale lze návod na interpretaci hledat též v rozsudku Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011, známém jako Kasalova pila. V tomto řízení šlo o určení neplatnosti výpovědi z pracovního poměru, kterého se domáhal zaměstnanec, jenž

---

[519] Op. cit. sub. 510, s. 24 a násl.
[520] Tamtéž.
[521] International Labour Office (ILO). Code of Pracite: Protection of workers‘ personal data. Geneva, International Labour Office, 1997. Čl. 6.14 a násl. [online]. [cit. 2019-04-19]. Dostupný z: https://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf

byl propuštěn z pracovního poměru za to, že během jednoho měsíce strávil na internetu více než 100 hodin činnostmi nesouvisejícími s výkonem jeho práce. Zaměstnavatel tuto skutečnost dokládal výpisem aktivit uživatelského loginu dotčeného zaměstnance, ze kterého bylo patrné, na jakých internetových stránkách se zaměstnanec pohyboval a jakou dobu tam strávil.

Nejvyšší soud přitom v daném řízení posuzoval skutečný smysl kontrol a dovodil, že *„cílem (smyslem) kontroly prováděné zaměstnavatelem (žalovaným) nebylo […] zjišťování obsahu e-mailových zpráv, obsahu SMS nebo MMS, případně odeslaných či přijatých zaměstnancem (žalobcem), nýbrž toliko zjištění, zda zaměstnanec (žalobce) respektuje […] zákaz užívat pro svou osobní potřebu výpočetní techniku zaměstnavatele […]".*[522] Nejvyšší soud následně částečně definoval, co lze ještě považovat za přiměřený způsob kontroly dle § 316 odst. 1 ZPr, když uvedl: *„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. […]; jde o důkaz pořízený v souladu se zákonem (s ustanovením § 316 odst. 1 větou druhou zák. práce)."*[523] Na daném rozhodnutí lze tedy ocenit, že Nejvyšší soud alespoň částečně naznačil, že při kontrolách dle § 316 odst. 1 ZPr je částečný zásah do soukromí přípustný. Negativně je nicméně nutné hodnotit skutečnost, že Nejvyšší soud se nijak nezaobíral porušením ochrany osobních údajů zaměstnance (byť by takové zkoumání nemuselo mít vliv na výsledek sporu).

Kromě toho rozhodnutí a rovněž rozhodnutí Nejvyššího soudu ze dne 7. srpna 2014, sp. zn. 21 Cdo 747/2013, které v podstatě případ Kasalova pila jen kopírovalo, nejsou v České republice v této otázce dostupná jiná rozhodnutí. Zajímavá rozhodnutí a odlišné přístupy lze však sledovat v zahraničí. Například německý federální pracovní soud (*Bundesarbeitsgericht)* v rozhodnutí ze dne 27. července 2017, sp zn. 2 AZR 681/16, dovodil, že použití důkazů získaných pomocí softwaru na evidování logů není při rozvázání pracovního poměru přípustné, pokud neexistuje podezření na trestný čin. Takové využití softwaru by tedy bylo přípustné pouze tehdy, pokud by zaměstnavatel měl konkrétní podezření na trestný čin zaměstnance nebo jiné závažné porušení jeho povinností. Je třeba však podotknout, že daný software byl schopen zaznamenávat veškeré dotyky s klávesnicí

[522] Rozsudek Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011.
[523] Tamtéž. Tento pohled Nejvyššího soudu byl též potvrzen v rozhodnutí NS ze dne 7. srpna 2014, sp. zn. 21 Cdo 747/2013.

a pravidelně pořizoval screenshoty zaměstnancovy obrazovky. V jiném rozhodnutí nicméně německý krajský pracovní soud (*Landesarbeitsgericht)* dospěl ve svém rozhodnutí ze dne 14. ledna 2016, sp. zn. 5 Sa 657/15, v podstatě ke stejnému závěru, k jakému dospěl náš Nejvyšší soud v případu Kasalova pila. V posuzovaném případě totiž rozhodl, že bylo oprávněné, pokud zaměstnavatel použil nástroj, na základě kterého zjistil, že zaměstnanec využíval svěřený počítač pro soukromé potřeby, a to více než 40 hodin ve sledovaném třicetidenním období.

Je tedy zřejmé, že i v Německu bude nutné posuzovat každý případ zvlášť na základě specifických skutkových okolností. Ve snaze, aby tyto případy byly posuzovány obdobně, vydal dozorový orgán v Meklenbursku-Pomořansku již v roce 2016 obsáhlou metodiku, co si zaměstnavatelé mohou a nemohou dovolit.[524] Lze tedy jen doufat, že se snad brzy také dočkáme obdobné metodiky ze strany českého dozorového orgánu, která by zohledňovala specifika ZPr.

8.1.4 GPS

Zcela odlišným nástrojem pro kontrolu a sledování zaměstnanců je využití GPS sledovacích systémů. Ty mohou zaměstnavatelé využívat zejména u svěřených automobilů či jiných dopravních prostředků, ale též u různých svěřených prostředků výpočetní techniky (mobily, počítače, tablety apod.). Odlišnost těchto nástrojů spočívá v tom, že umožní zaměstnavateli sledovat obvykle jediný specifický druh jednání zaměstnanců, kterým je jejich pohyb (některé systémy dnes jdou však již dále a umějí například zaznamenávat různé prvky chování řidiče apod.). I přesto bude moci zaměstnavatel na základě takových dat za určitých okolností dovodit další skutečnosti (jaké jsou zvyky zaměstnance, kde tráví polední pauzu, kam chodí nakupovat apod.). Právě i proto se na tyto kontrolní a sledovací nástroje bezesporu rovněž plně uplatní pravidla obsažená v ustanovení § 316 odst. 1 ZPr (pro potřeby ochrany majetku zaměstnavatele prostřednictvím namátkových kontrol) a § 316 odst. 2 ZPr (pro potřeby soustavného sledování zaměstnanců). Nezbytností bude samozřejmě uplatnění

[524] Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern: *Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz*. Januar 2016 [online]. [cit. 2019-04-30]. Dostupné z: https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/oh-internet-arbeitsplatz.pdf

pravidel na ochranu osobních údajů, neboť získané informace půjde vždy vztáhnout ke konkrétnímu zaměstnanci.[525]

K aplikaci těchto pravidel při využití GPS sledovacích systémů již v praxi došlo ze strany ÚOOÚ, který posuzoval zákonnost využití tohoto nástroje na sledování zaměstnanců za účelem optimalizace doručování. V rozhodnutí ze dne 3. 7. 2013, č. j. UOOU-00237/13-38, přitom uzavřel, že *„považuje soustavné sledování zaměstnanců za účelem optimalizace doručovacích okrsků (resp. vyřizování reklamací) za závažný a zcela nedůvodný zásah do jejich soukromí, aniž by, jak již bylo uvedeno výše, účastník řízení využil možnosti, které jsou z hlediska soukromí méně invazivní a které nepochybně existují, popř. se omezil na využití technologie v omezeném rozsahu (jednorázové či krátkodobé v řádu několika dnů).* Úřad tak upozornil na nutnost aplikovat princip subsidiarity a využít jiné mechanismy, lze-li jejich pomocí dosáhnout sledovaného účelu, a zároveň též na princip proporcionality (jsou-li již tyto nástroje, mělo by jejich využití být omezeno na nezbytné minimum). Úřad zároveň správně a s ohledem na rozsah kontrolních využití těchto prostředků dovodil nutnost aplikace § 316 odst. 2 ZPr a zároveň konstatoval, že pro takovýto postup v daném případě neexistovaly závažné důvody spočívající ve zvláštní povaze činnosti zaměstnavatele.

U využití GPS sledovacích systémů však mohou nastat některé specifické situace. V případě zaměstnanců dopravy, resp. dopravních firem, jde o běžnou záležitost, která byla též aprobována ze strany WP29, neboť zaměstnavatelé obvykle nejen chrání svůj majetek, ale též musí dohlížet na dodržování zákonných povinností týkajících se bezpečnosti (zejména povinné přestávky).[526] Je otázkou, zda bude nutné i na tyto případy v takové situaci aplikovat ustanovení § 316 ZPr. WP29 uzavřela, že takovéto mechanismy nejsou zařízeními pro sledování zaměstnanců (a jejich funkcí je sledování lokace vozidel).[527] Tato domněnka však nezabrání zaměstnavatelům tyto údaje použít též proti zaměstnanci, bude-li to nutné, a proto by se podle názoru autora této práce měla ochrana dle § 316 odst. 1 a 2 ZPr plně aplikovat, byť v určité nižší míře.

Naopak plně by se tato ustanovení měla aplikovat na ostatní případy, kdy je zaměstnancům svěřeno vozidlo či jiné zařízení umožňující sledování pomocí GPS. ÚOOÚ

---

[525] To potvrdil i ÚOOÚ, který dovodil, že „*osobním údajem je jakákoli informace, která se týká konkrétní fyzické osoby, což nepochybně informace o pohybu zaměstnance splňuje (s tím nijak nesouvisí, jakým způsobem lze s takovým údajem nakládat)*“ (srov. rozhodnutí ÚOOÚ ze dne 3. 7. 2013, č.j. UOOU-00237/13-38).

[526] Stanovisko WP29 č. 2/2017: Zpracování údajů na pracovišti (v originále: *opinion 2/2017 on data processing at work*). (WP249), ze dne 8. června 2017, s. 20.

[527] Stanovisko WP29 č. 13/2011: Ke geolokalizačním službám u inteligentních mobilních zařízení (v originále: *opinion 13/2011 on Geolocation services on smart mobile devices*). (WP185), ze dne 16. května 2011, s. 14.

nicméně dále dovozuje, že *„monitorování služebních vozidel při pracovních cestách pomocí GPS v rozsahu a způsobem potřebným pro ochranu a správu majetku je oprávněným zájmem zaměstnavatele, tedy zpracováním osobních údajů dle článku 6 odst. 1 písm. f) GDPR“.*[528] Úřad je tedy v tomto ohledu relativně benevolentní a za správce obecně provedl balanční test pro tyto potřeby.[529] Dokonce dále považuje za oprávněný zájem zaměstnavatele, pokud je GPS sledování zapnuté i v případě, kdy zaměstnanec využívá vozidlo pro své osobní potřeby.[530] Naopak WP29 se domnívá, že tyto důvody obvykle dány nebudou a dovozuje, že tato funkce by měla být v takových případech obvykle vypnuta.[531] Autor této práce se v tomto případě spíše přiklání k názoru WP29.

Jak již bylo naznačeno, kromě zaznamenávání pohybu pomocí GPS dnes také mnohdy platí, že sledovací zařízení v automobilech umožňují shromažďovat i další informace, jako je chování řidiče, přičemž tyto systémy se umí sepnout jen v případě neobvyklé události (například náhlé brždění). Může jít rovněž o kamery zaznamenávající okolí. WP29 tyto nástroje označuje za zapisovače událostí a dovozuje legálnost jen při nezbytnosti jejich zpracování, která bude dána obvykle u organizací zabývajících se přepravou.[532] Podle názoru autora této práce bude na takovéto systémy nutné aplikovat závěry v předchozím bodě 8.1.3, a tedy bude záviset na míře, v jaké budou zasahovat do soukromí jednotlivců, a na základě toho bude nutné ad hoc vyhodnocovat zákonnost jejich použití.

8.1.5 Kamery

Patrně nejintenzivnějším nástrojem pro sledování zaměstnanců, který připadá do úvahy, je využití kamerových systémů na pracovišti. S určitými obavami pak lze hodnotit, že nejde o nástroj zcela neobvyklý. Na úvod je vhodné poznamenat, že z hlediska ochrany osobních údajů je nutné podle názoru ÚOOÚ rozlišovat, kdy je kamerový systém provozován se záznamem a kdy je provozován bez něj. Úřad totiž dovodil, že v případě, že

---

[528] ÚOOÚ: Sekce: často kladené dotazy. *Zaměstnavatelé. Lze monitorovat služební vozidla pomocí GPS?* [online]. [cit. 2019-04-15]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5057&n=zamestnavatele

[529] Tento názor v zásadě akceptoval i Nejvyšší soud ČR, který ve svém rozhodnutí ze dne 7. června 2017, sp. zn. 21 Cdo 817/2017, dovodil přiměřenost kontroly používání prostředků zaměstnavatele (dle § 316 odst. 1 ZPr) i na případ sledování svěřeného vozidla pomocí GPS zařízení.

[530] Tamtéž. Úřad ale zdůrazňuje, že i tak je ale nutné zpracovávat získané osobní údaje výhradně v mezích definovaných účelů, jako je evidence knihy jízd, odpisy vozidla, bezpečnostní přestávky apod.

[531] Stanovisko WP29 č. 2/2017: Zpracování údajů na pracovišti (v originále: *opinion 2/2017 on data processing at work).* (WP249), ze dne 8. června 2017, s. 17.

[532] Tamtéž, s. 17 a 18.

není pořizován záznam, nejedná se o zpracování osobních údajů.[533] Úřad se nicméně v tomto svém stanovisku odkazoval na ustanovení § 4 písm. e) ZOOÚ, které v rámci definování pojmu „zpracování“ explicitně nezmiňovalo nahlédnutí. Naopak nařízení GDPR ve svém čl. 4 bod 2) uvádí, že za zpracování je možné považovat již pouhé nahlédnutí.

Je tedy otázkou, zda dříve vydané stanovisko obstojí i v době účinnosti GDPR. Ostatně ani WP29 nedovozovala tak kategorické závěry jako ÚOOÚ, ale poměřovala využití záznamů a online sledování jen v rámci výkladu o proporcionalitě a shledala, že online sledování bez záznamů by mělo být využívané například na pokladnách v supermarketu, kde bude dostatečné pro stanovený účel (i tak ale jde o zpracování osobních údajů).[534] Podle názoru autora této práce bude v případě online sledování rozhodné, jaký je záměr takového provozování kamer. Pokud je jím soustavný dohled nad zaměstnanci, měla by být taková činnost považována spíše za zpracování osobních údajů.[535] Obdobně Nulíček, který v této souvislosti dovozuje, že pro vyhodnocení určité činnosti jako zpracování je rozhodné, jaký je účel takové činnosti. Pokud je jím práce s daty, pak jde o zpracování. Naopak pokud je přístup k datům jen náhodný či nepravidelný, o zpracování se nejedná.[536] V posuzovaném případě by tedy bylo možné uzavřít, že účelem je práce s daty spočívající v tom, že jiný zaměstnanec kameru sleduje a obraz vyhodnocuje (a nejde tedy o náhodnou činnost). Bude však zajímavé, jak se k této otázce postaví ÚOOÚ. Zatím nenasvědčuje nic tomu, že by svůj postoj měl změnit.

Z hlediska ochrany osobních údajů je třeba ještě uvést, že aby šlo o zpracování osobních údajů, musí být na kameře určitá identifikovaná či identifikovatelná osoba. V případě využití kamer se přitom nemusí jednat jen o situace, kdy bude osoba rozpoznatelná podle obličeje či jiných zjevných prvků, ale může jít též o případy, kdy bude rozpoznatelná podle prvků chůze, oblečení, chování apod. WP29 jde ještě dál a dovozuje, že osoba bude identifikovatelná například ve spojitosti s tím, že zadá do systému PIN (aniž by byl nahrán obličej osoby), nebo podle registrační poznávací značky. Omezení nejsou

---

[533] Srov. stanovisko ÚOOÚ č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Leden 2006.

[534] Srov. stanovisko WP29 č. 4/2004: Ke zpracování osobních údajů prostřednictvím kamerového sledování (v originále: *opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*). (WP89), ze dne 11. února 2004, s. 20.

[535] Pro úplnost je nutné podotknout, že tyto závěry mohou mít význam i pro jiné sledovací nástroje. Například nástroj, který pouze zrcadlí obrazovku zaměstnance a jedna ku jedné ji zobrazuje na jiném zařízení, aniž by z toho byl pořizován záznam, by ve světle stanoviska ÚOOÚ také neměl být považován za zpracování osobních údajů.

[536] Srov. Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017, s. 86.

kladena ani z hlediska využití typů kamer (barevné či černobílé, drátové či bezdrátové, stacionární či mobilní) a způsobů nahrávání (kontinuální záznam či při výskytu události).[537]

Bez ohledu na to, jestli půjde o zpracování osobních údajů či nikoliv, je třeba konstatovat, že využití jakéhokoliv kamerového systému na pracovišti představuje značný zásah do soukromí jedinců. Podle názoru autora této práce by měly být kamery na pracovišti využívány jen v případech předvídaných v rámci ustanovení § 316 odst. 2 ZPr. V případě kontrol toho, zda zaměstnanci řádně využívají svěřené výrobní a pracovní prostředky ve smyslu § 316 odst. 1 ZPr, nebude totiž podle názoru autora této práce obvykle možné označit využití kamer za přiměřený způsob kontroly.[538] Aby bylo možné uvažovat o zákonnosti provozování kamerového systému, měly by proto být u zaměstnavatele dány závažné důvody spočívající ve zvláštní povaze činnosti zaměstnavatele.

V podobném duchu vyznívají též dostupná rozhodnutí vyšších soudů. Například Nejvyšší správní soud ČR se ve svém rozhodnutí ze dne 23. srpna 2013, sp. zn. 5 As 158/2012, zabýval otázkou zákonnosti umístění kamerového systému v hotelu a souvisejícího sledování zaměstnanců a jasně se vyjádřil, že pro zákonnost kamerového systému je nutné využít výjimku danou ustanovení § 316 odst. 3 ZPr. V této souvislosti dále uvedl, že *„k instalaci kamerových systémů, s ohledem na jejich povahu a zásah do osobní integrity osob, je možné přistoupit až tehdy, pokud už veškeré méně invazivní prostředky selhaly anebo by nebyly schopny naplnit vytyčený účel, který je sledován. Je zcela nepochybné, že kamerový systém ve srovnání s jinými prostředky (např. personálními, mechanickými), které mohou dosáhnout naplnění účelů žadatelem sledovanými, zasahuje základní lidská práva, a to právo na soukromí a na soukromý rodinný život, která jsou garantována čl. 10 Listiny základních práv a svobod a v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod, a tudíž i do lidské důstojnosti, z které tato práva vyplývají.“*.[539] Zajímavé jsou rovněž dále podané závěry: *„Monitoring zaměstnance je možný pouze na základě předchozího oznámení a jen tam, kde je to nezbytné k ochraně zdraví osob nebo majetku zaměstnavatele. Monitoring musí být směřován na majetek*

[537] Op. cit. sub. 534, s. 15.
[538] Shodně se vyjadřuje též Státní úřad inspekce práce (op. cit. sub. 265). Výjimkou by patrně mohla být situace, kdy zaměstnavatel má konkrétní podezření na nelegální činnost zaměstnance a za účelem prověření takové situace dočasně nainstaluje kamerový systém. Přípustnost tohoto postupu byla shledána v rozhodnutí ESLP ze dne 5. října 2010 ve věci Köpke vs. Německo, č. stížnosti 420/07, v rámci kterého soud dovodil, že nahráváním zaměstnance na pracovišti (kterým byla pokladna v supermarketu) bez předchozího oznámení a následné využití získaných informací v soudním sporu může být přípustné, pokud bylo provedeno v omezeném časovém období a na základě předchozího podezření o nepoctivém jednání zaměstnance.
[539] Rozhodnutí Nejvyššího správního soudu ČR ze dne 23. srpna 2013, sp. zn. 5 As 158/2012.

zaměstnavatele, nikoliv na osobu zaměstnance (nasměrování kamer) a musí být prováděn na pracovišti, nikoliv na místech určených k hygieně nebo k odpočinku zaměstnance. Předmětem informace zaměstnanci před započetím monitoringu je rovněž rozsah a způsob provádění kontroly.“[540]

Na nutnost hledat závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele poukázal Nejvyšší správní soud také v rozhodnutí ze dne 20. prosince 2017, sp. zn. 10 As 245/2016, v rámci něhož uzavřel, že tato podmínka není obecně naplněna u řidiče autobusu. V souvislosti s výkladem o kamerových systémech nelze opomenout také již zmiňované nedávné rozhodnutí ve věci *Antonović a Mirković vs. Černá hora*,[541] v rámci kterého bylo dovozeno, že i když zaměstnavatel zaměstnance o kamerovém systému informuje, neznamená to automaticky, že využití takového systému je v souladu se zákonem. To v zásadě odpovídá závěrům, které je nutné dovodit v rámci českého právního řádu s odkazem na § 316 odst. 2 a 3 ZPr.

Zaměstnavatel samozřejmě před instalací kamerového systému bude povinen splnit celou řadu dalších povinností. Těmi je zejména informování o kamerovém systému a o zpracování osobních údajů, informování o podmínkách využití takového kamerového systému, provedení balančního testu[542] a obvykle též provedení posouzení vlivu na ochranu osobních údajů.[543] V té souvislosti bude muset zaměstnavatel důkladně posoudit, jaký kamerový systém (a zda vůbec nějaký) je schopný naplnit sledované účely, zda neexistuje mírnější opatření, zda nebude nad míru zasahovat do práva na ochranu soukromí zaměstnanců, zda jsou záznamy dostatečně zabezpečeny, zda není zamýšlená doba uchování záznamů příliš dlouhá, tj. zda je dostatečná pro vyhodnocení pořízených záznamů (podle ÚOOÚ by doba uchování záznamů obvykle neměla překračovat dobu několika dnů[544]) atd.

S ohledem na výše uvedené je jen s podivem, že v poslední době neustále dochází k obecnému nárůstu instalovaných kamer. Autor této práce má značné pochybnosti

---

[540] Tamtéž. K obecné otázce využitelnosti kamerových systémů lze dále odkázat na závěry v rozhodnutí Nejvyššího správního soudu ČR ze dne 25. února 2015, sp. zn. 1 As 113/2012, či ze dne 28. června 2013, sp. zn. 5 As 1/2011. V těchto případech však nebyla posuzována aplikace ustanovení § 316 ZPr.

[541] Rozhodnutí ESLP ze dne 28. listopadu 2017 ve věci Antonović a Mirković v. Černá hora, č. stížnosti 70838/13.

[542] Prakticky jediným vhodným právním základem pro zpracování osobních údajů bude v této situaci oprávněný zájem zaměstnavatele ve smyslu čl. 6 odst. 1 písm. f) GDPR, který provedení balančního testu vyžaduje. Výjimkou mohou být situace, kdy je provozování kamerového systému uloženo zákonem. Naprosto nevhodným právním základem v této situaci však nepochybně je souhlas zaměstnanců.

[543] Srov. závěry podané v bodě 7.7.3.

[544] Srov. stanovisko ÚOOÚ č. 1/2006: *Provozování kamerového systému z hlediska zákona o ochraně osobních údajů*. Leden 2006.

o skutečnosti, že ve všech těchto případech jsou splňovány výše uvedené podmínky, jako jsou závažné důvody spočívající ve zvláštní povaze činnosti zaměstnavatele, řádné informování, balanční test či posouzení vlivu na ochranu osobních údajů. Do doby, než začnou být tyto situace důsledněji monitorovány a přísněji sankcionovány ze strany dozorových orgánů, však zaměstnavatele těžko něco přinutí, aby od tohoto chování ustoupili.

8.2 Whistleblowing

Alespoň okrajově je vhodné se v této práci vyjádřit též k otázce whistleblowingu, tedy k činnosti, která spočívá v ohlašování nezákonné či protiprávní činnosti jiných zaměstnanců či zaměstnavatele.[545] Tato otázka je velmi důležitá z hlediska ochrany soukromí a osobních údajů ohlašovatele (zaměstnance), ale může mít samozřejmě význam též z hlediska ochrany osoby obviněné z protiprávního jednání. Ačkoliv jde o relativně nový fenomén, jeho vznik je možné hledat již v 70. letech 20. století[546] a již v roce 2006 k této otázce vydala WP29 své stanovisko ohledně přípustnosti z hlediska ochrany osobních údajů.[547]

Závěry podané v tomto stanovisku lze shrnout tak, že zpracování osobních údajů v případě zavedení whistleblowingu bude vždy možné podřadit pod oprávněný zájem zaměstnavatele (případně též pod plnění právní povinnosti, existuje-li taková). Z hlediska zákonnosti zpracování je důležitá dále otázka aplikace ostatních zásad včetně transparentnosti (povinnosti informovat o způsobech zpracování) či proporcionality (zpracovávat osobní údaje jen v nezbytném rozsahu a po nezbytnou dobu). Ač by se na první pohled mohlo zdát, že tomu bude naopak, WP29 podporuje podávání podepsaných (nikoliv anonymních) oznámení, a to zejména z důvodu vyšší možnosti prošetření, a tedy vyšší pravděpodobnosti dosažení sledovaného účelu. Patrně nejzásadnější je pak zajištění

---

[545] Lze dohledat i širší definice. Například Morávek a Pichrt vztahují oznamování k jakémukoliv jednání, *„které je v rozporu se zákonem, veřejným pořádkem, dobrými mravy, morálkou či politikou nebo strategií dané entity, a které je v rámci oznamovacích mechanismů označeno jako relevantní a škodlivé*“ (srov. Pichrt, J., Morávek, J. *Whistleblowing*. Právo pro podnikání a zaměstnání. 2009, 18(7-8), s. 19.). Není však záměr v této práci hledat přesnou definici, ale zaměřit se na způsob ochrany soukromí a osobních údajů zaměstnanců.

[546] Perry, N. Indecent Exposures: Theorizing Whistleblowing. Department of Sociology. The University of Auckland, New Zealand, Volume: 19 issue: 2, page(s): 235-257, Publikováno 1. března 1998, s. 235. [online]. [cit. 2018-05-04], Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.923.9031&rep=rep1&type=pdf

[547] Stanovisko WP29 č. 1/2006: K aplikaci pravidel ochrany osobních údajů na whistleblowing (v originále: *opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime)*. (WP117), ze dne 1. února 2006.

odpovídající ochrany osobních údajů v užším smyslu, tj. zajištění odpovídajícího utajení. Především je nutné zajistit, aby se oznamované skutečnosti dostaly k pověřeným osobám, nebyly zneužity, případně aby nebyly použity proti oznamovatelům.

Vhodným základem pro řádné fungování schémat whistleblowingu je jejich legislativní úprava. V českém právním řádu existuje komplexní úprava zatím pouze ve vztahu k zaměstnancům ve státní službě, a to v rámci nařízení vlády č. 145/2015 Sb., o opatřeních souvisejících s oznamováním podezření ze spáchání protiprávního jednání ve služebním úřadu. Vedle toho je též ve vybraných předpisech uložena povinnost zavést systémy pro whistleblowing (interní hlášení) pro některé specifické subjekty.[548] V ostatních případech se však zaměstnanci nemohou spolehnout na zákonem jasně definovaný rámec, který by zajišťoval jejich ochranu pro případ učiněného oznámení.

V současné době je nicméně opět chystán (obecný) návrh zákona o ochraně oznamovatelů, který by toto mohl změnit.[549] Klíčovými prvky tohoto návrhu je, že by se měl vztahovat obecně na veškeré zaměstnavatele (pokud jde o soukromé subjekty má se tato povinnost týkat těch, kteří splňují určitá kritéria, například více než 50 zaměstnanců, určitý limit ročního obratu, veřejné zadavatele apod.), že by u Ministerstva spravedlnosti měla být zřízena agentura na ochranu oznamovatelů, oznámení by bylo možné činit vnitřní formou (u zaměstnavatele) či vnější (u stanoveného orgánu). Protiprávním jednáním by se přitom dle tohoto návrhu měly rozumět trestný čin, přestupek a jednání, které má znaky trestného činu nebo přestupku. Návrh samozřejmě předpokládá zákaz jakýchkoliv odvetných opatření vůči oznamovateli a garanci ochrany jeho totožnosti.

Kromě návrhu českého zákona je nutné zmínit, že v současné době je na půdě Evropského parlamentu a Rady též chystán návrh směrnice o ochraně osob oznamujících porušení práva Unie, jejímž cílem je dokonce sjednotit ochranu oznamovatelů napříč Evropskou unií.[550] Také návrh této směrnice má být obecný a vztahovat se na subjekty ve veřejném i soukromém sektoru (u soukromých opět na základě určitých kritérií, které jsou

---

[548] Například pro banky, spořitelní a úvěrová družstva či obchodníky s cennými papíry, a to v rámci vyhlášky č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry, nebo pro pojišťovny (srov. ustanovení § 48 odst. 1 písm. e) zákona č. 170/2018 Sb., o distribuci pojištění a zajištění).
[549] Návrh zákona o ochraně oznamovatelů. Předkladatel: Ministerstvo spravedlnosti, č.j. OVA 140/19. Elektronická knihovna připravované legislativy pro veřejnost [online]. [cit. 2019-05-06]. Dostupné z: https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=3&_material_WAR_odokkpl_pid=ALBSB9HFJX37&tab=detail
[550] Návrh směrnice Evropského parlamentu a Rady o ochraně osob oznamujících porušení práva Unie, COM/2018/218 final – 2018/0106.

zatím podobné kritériím v návrhu českého zákona), předpokládá vytvoření externích či vnějších kanálů pro oznamování a zavádí důslednou ochranu oznamovatelů včetně zákazu odvetných opatření (ta je dokonce podrobnější než v návrhu českého zákona).

Je tedy otázkou, do jaké míry má význam projednávání a schvalování českého návrhu zákona, který ne ve všech ohledech odpovídá požadavkům připravované směrnice (ač jí zároveň v určitých ohledech odpovídá). Ať už tento legislativní závod dopadne jakkoliv, lze bezpochyby očekávat, že ochrana zaměstnanců bude tímto krokem dále posílena. Toto je třeba nepochybně kladně hodnotit. Zaměstnanci by se napříště neměli oznamování v žádném ohledu obávat, jelikož by měla být dostatečně garantována ochrana jejich soukromí a zpracování osobních údajů. Takové prostředí nepochybně přispěje k dosažení cílů whistleblowingu, kterými není jen efektivní boj proti korupčnímu jednání, ale též boj proti jiným případům jednání proti dobrým mravům či jednání porušujícím zákon, veřejný pořádek, nebo dokonce interní pravidla zaměstnavatele.

8.3 Odhalování majetku zaměstnanců

V praxi se lze setkat se situacemi, kdy zaměstnavatelé vyžadují, či si dokonce sami skrytě zjišťují informace o majetku svých zaměstnancům. To neplatí jen v souvislosti se vznikem pracovního poměru, ale zejména v době jeho trvání. Takové jednání bývá často zaměstnavateli odůvodňováno rizikem toho, že by zaměstnanec s ohledem na své postavení mohl této skutečnosti zneužívat a zaměstnavatele či jiné třetí osoby nezákonně připravovat o majetek. Takové jednání zaměstnance by přitom nemuselo být zjistitelné s pomocí sledovacích prostředků, neboť by zejména mohlo spočívat pouze v předávání informací zaměstnancem jiným osobám, které by této znalosti využívali pro nezákonné obohacení. Může se přitom jednat o relativně širokou škálu informací, od těch, které by umožnily fyzické odcizení majetku, až po ty, které by umožnily zneužití vnitřních informací či jiné formy zneužívání trhu. Záměrem popsaného prověřování majetku zaměstnanců je pak zjišťování, zda nedochází k neúměrnému obohacování zaměstnance, aniž by to bylo odůvodnitelné s ohledem na příjmy daného zaměstnance, neboť by to následně mohlo vzbudit pochybnosti, zda na straně zaměstnance nedochází k určité nezákonné činnosti.

Podle názoru autora této práce je tento přístup velmi závažný a mělo by k němu docházet opravdu jen v naprostém minimu odůvodněných případů, kdy na straně

zaměstnavatele existuje určitý veřejný zájem či jiný velmi závažný důvod.[551] Taková činnost do značné míry již supluje pravomoci orgánu policie či jiných bezpečnostních sborů, k čemuž by rozhodně nemělo docházet. I z hlediska zákonnosti takového postupu bude velmi obtížné nalézt argumenty pro zákonnost takového postupu. Z hlediska ZPr lze v tomto ohledu argumentovat s odkazem na ustanovení § 316 odst. 4 ZPr,[552] které omezuje právo zaměstnavatele vyžadovat informace o rodinných a majetkových poměrech zaměstnance na situace, kdy je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li takový požadavek přiměřený, případně ukládá-li takový postup zákon. V žádném případně již navíc není umožněno, aby si zaměstnavatel tyto informace zjišťoval sám.

Z hlediska zpracování osobních údajů je situace ještě komplikovanější z hlediska identifikace právního základu, na němž by měla být postavena zákonnost zpracování takto zjištěných informací. Pomineme-li možnost, že by takové zpracování ukládal zákon, zbývá jen právní základ spočívajícím na oprávněném zájmu zaměstnavatele (případně třetí osoby). Takový právní základ by si však vyžádal provedení balančního testu se všemi jeho náležitostmi. To znamená, že by zejména musela být nalezena odpověď na otázku, zda je takové opatření či zpracování osobních údajů skutečně schopné dosáhnout sledovaného účelu. O tom lze mít značné pochybnosti, pokud nebude kromě zaměstnancova majetku sledován též majetek všech jeho osob blízkých. Avšak už ve vztahu k samotnému zaměstnanci se jedná podle názoru autora této práce o tak závažný zásah do soukromí zaměstnance, že zákonnost takovéhoto zpracování bude v naprosté většině případů vyloučena.

[551] Jako příklad by se mohla nabízet práce osoby pracující se snadno zneužitelnými (zpeněžitelnými) informacemi.

[552] Sporná může být otázka aplikace tohoto ustanovení na popsaný případ zjišťování informací za trvání pracovního poměru, když obecně by mělo toto ustanovení mířit na informace, které zaměstnavatel vyžaduje v souvislosti s náborem zaměstnanců. Podle názoru autora práce je však použití dotčeného ustanovení na popisovaný případ možné.

9 Komparativní pohled a zamyšlení de lege ferenda

Záměrem této kapitoly je stručný rozbor nejzajímavějších zahraničních právních úprav věnujících se otázkám zkoumaným v rámci této práce. Není však cílem zabývat se detailně jednotlivými výkladovými otázkami těchto právních úprav, ale spíše jen poukázat na možnosti legislativního řešení. To zároveň poslouží pro druhou podkapitolu, která se následně s ohledem na dříve podaný výklad zamýšlí nad nejspornějšími otázkami ochrany soukromí a osobních údajů na pracovišti, kriticky hodnotí současnou právní úpravu a snaží se nabídnout pohled autora této práce na možné budoucí legislativní řešení.

9.1 Komparativní pohled

V bodě 4.1.1 již byla částečně vyzdvihnuta ochrana soukromí zaměstnanců poskytovaná ve Finsku, a to ve vztahu k uchazečům o zaměstnání. Tamní zákon na ochranu soukromí v pracovním životě[553] ale stojí za pozornost i z jiných hledisek a fází vztahu mezi zaměstnancem a zaměstnavatelem. Především je explicitně zmíněno, že zaměstnavatelé jsou oprávnění zpracovávat jen údaje, které jsou přímo nezbytné pro pracovněprávní vztah a jeho správu. Dále je specificky omezeno zpracování osobních údajů týkajících se zdraví na případy, kdy musí zaměstnavatel platit náhrady spojené s nemocí nebo posuzovat, zda je absence zaměstnance omluvitelná, nebo je posuzována pracovní schopnost zaměstnance (a to na základě zaměstnancova požadavku). V souvislosti s údaji o zdraví je zaměstnavatel rovněž povinen organizačně (jmenováním konkrétní odpovědné osoby) a technicky zajistit, že bude zajištěno utajení těchto informací. Obdobné povinnosti platí v případě informací týkajících se užívání drog či léčiv, resp. související způsobilosti k práci, a to specificky pro nábor zaměstnance i za dobu trvání pracovněprávního vztahu, kdy má zaměstnavatel podezření na užívání drog ze strany zaměstnance. Specificky je též upraveno, za jakých podmínek může být zkoumána zaměstnancova osobnost a schopnost vykonávat nabízenou práci.

Zvláštní kapitola tohoto zákona se věnuje též využití kamer na pracovišti. Předně jsou jasně omezeny účely, pro které lze takové sledování zavést. Těmi je bezpečnost zaměstnanců a jiných osob na pracovišti, ochrana majetku a dohled nad výrobním procesem či vyšetřování situací ohrožujících bezpečnost, majetek či výrobní proces. V žádném případě

[553] Act on the Protection of Privacy in Working Life (759/2004). © Ministry of Labour, Finland. [online]. [cit. 2019-05-08]. Dostupné z: https://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf

však kamery nemohou být využity pro sledování konkrétního zaměstnance či zaměstnanců na pracovišti. Nesmějí být umisťovány ani ve specifických prostorách, jako jsou toalety, šatny či jiná obdobná místa. I tak však existují výjimky, kdy zaměstnavatel může využít kamerový systém sledující konkrétní pracoviště (vyšetřování trestných činů, ochrana před zjevným nebezpečím či pro ochranu zdraví zaměstnance nebo na základě výslovného přání zaměstnance). Samozřejmostí je před zavedením kamerového systému provedení balančního testu, přičemž tento zákon vyjmenovává konkrétní aspekty, které je nutné zohlednit. Specificky je zaměstnavatel oprávněn využít kamerové záznamy pro rozvázání pracovního poměru, vyšetřování obtěžování na pracovišti či vyšetřování hrozby pro zdraví zaměstnanců.

Zvláštní kapitola je věnována též sledování elektronické komunikace zaměstnanců (na prostředcích zaměstnavatele). V tomto ohledu jsou však nastaveny jasné a detailní podmínky, za kterých může zaměstnavatel takovou elektronickou komunikaci otevřít. Předně musí zaměstnanci umožnit, aby mohl sám aktivně předejít situacím, kdy bude zaměstnavatel nucen otevírat jeho poštu – zejména možností nastavení *out of office*, možností přeposílání jinému určenému zaměstnanci apod. Dále musí být v případě otevírání zaměstnancových e-mailů přítomen IT administrátor a musí jít jen o skutečně nezbytné případy, kdy je zřejmé, že zaměstnavateli hrozí škoda z důvodu, že na e-maily nebude reagováno (a rovněž nelze získat zaměstnancův souhlas s otevřením takové pošty).

Při porovnání tohoto finského zákona s podobnou legislativou v jiných zemích, je zřejmé, že finská legislativa je v podstatě nejpřísnější ze všech a zaměstnanci ve Finsku si užívají jednu z nejvyšších úrovní ochrany svého soukromí. To však neznamená, že by ochrana zaměstnanců v jiných zemích nestála za pozornost. Například německý zákon o ochraně osobních údajů (BDSG)[554] obsahuje samostatné ustanovení týkající se zpracování osobních údajů zaměstnanců (čl. 26). Byť jde o jediné ustanovení, je poměrně obsáhlé a obsahuje relativně hodně specifických pravidel. Předně je omezen okruh případů či účelů, při kterých jsou zaměstnavatelé osobní údaje zpracovávat (nábor, plnění pracovní smlouvy, pro naplnění a výkon práv souvisejících se zastupováním zaměstnancům v kolektivních pracovněprávních vztazích, prošetření podezření na spáchání trestného činu). BDSG se též vyjadřuje k možnosti zpracování na základě souhlasu zaměstnance, přičemž zdůrazňuje, že v takovém případě musí být důkladně posuzována platnost souhlasu s ohledem na závislost

[554] Bundesdatenschutzgesetz (BDSG) z 30. června 2017 (BGBl. I S. 2097) [online]. [cit. 2019-05-08]. Dostupný z: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0222

zaměstnance a okolnosti, za nichž byl souhlas udělen. Platné udělení souhlasu se předpokládá zejména tehdy, pokud jeho udělení bude spojeno s právním či ekonomickým benefitem pro zaměstnance. Pro souhlas se obecně vyžaduje písemná či jiná vhodná forma, přičemž jeho obsahem musí být poučení o možnosti jeho odvolání.

BDSG se věnuje též specifickým otázkám souvisejícím se zpracováním zvláštních kategorií údajů nebo vymezuje podmínky aplikace tohoto zákona. Za zmínku stojí též ustanovení čl. 26 odst. 4 BDSG, které předpokládá, že bližší pravidla zpracování osobních údajů budou upravena také v kolektivních smlouvách. To je jistě velmi zajímavý instrument, kterým lze v celé řadě případů dohnat určité legislativní nedostatky, resp. pro konkrétního specifického zaměstnavatele vymezit, co se pod obecnými pojmy ukrývá a jak mají být vykládány u daného zaměstnavatele.

Cestou kolektivních smluv se vydala též Belgie, a to dokonce již na národní úrovni. V Belgii totiž existují národní kolektivní smlouvy, které upravují specifické otázky sledování zaměstnanců. Jde konkrétně o Národní kolektivní smlouvu č. 68, týkající se použití kamer na pracovišti, a Národní kolektivní smlouvu č. 81, týkající se sledování elektronických komunikací.[555] Na základě těchto kolektivních smluv jsou vymezeny podmínky a pravidla, kdy a jak může zaměstnavatel monitorování provádět. Zejména jen v situacích, kdy neexistuje méně invazivní nástroj pro dosažení sledovaného cíle. Nahrávky hovorů zaměstnanců mohou být pořizovány jen pro potřeby ověření, že je dostatečně kvalitně poskytována služba. Otevřít e-maily zaměstnance lze jen v případě, pokud je zaměstnanec nedostupný, aby byla zajištěna kontinuita poskytování služeb.

V případě kamerových systémů pak platí, že mohou být pro potřeby přímého sledování zaměstnanců využity výhradně po omezeně krátkou dobu. Pravidla v kolektivních smlouvách se týkají též využití docházkových systémů či geolokačních systémů. Obecně je dále definováno, že sledování ze strany zaměstnavatele může být využíváno, jen pokud slouží (i) k prevenci nezákonného či neetického jednání, (ii) ochraně ekonomických a finančních zájmů zaměstnavatele, (iii) zajištění řádného fungování IT sítě zaměstnavatele

[555] Kuschewsky, M. *Data Protection & Privacy, Jurisdictional comparisions.* First edition. London. Sweet & Maxwell, part of Thomson Reuters, 2012, a osobní konzultace s vybranými právními poradci z různých evropských zemí v rámci konference WSG (World Services Group) v Lisabonu, Portugalsko, konané dne 21. a 22. března 2019.

nebo (iv) k zajištění dodržování principů a pravidel týkajících se využívání online technologií.[556]

Podíváme-li se mimo Evropskou unii, stojí za zmínku například Norsko, které se rovněž snaží zajistit zaměstnancům dostatečnou ochranu. Tamní zákon o pracovním prostředí[557] obsahuje samostatný článek 9, týkající se zavedení kontrolních opatření u zaměstnavatelů. Především se uvádí, že zaměstnavatel je oprávněn sledovací prostředky zavést pouze tam, kde je to oprávněné okolnostmi a nepředstavuje nedůvodnou zátěž pro zaměstnance. Rovněž je vyzdvihnut princip privacy by design a nutnost před zavedením takovýchto systémů je konzultovat přímo se zaměstnanci (to se týká též změn těchto systémů a jejich vyhodnocování v čase). Rovněž je blíže uvedeno, o čem všem by měl zaměstnavatel své zaměstnance informovat v souvislosti se zavedením těchto systémů (účely, důsledky zavedení a jak budou vyhodnocovány, předpokládaná doba trvání). Zvláštní úprava se týká též možnosti vyžadování informací o zdravotním stavu při náboru.

Pokud jde o možnosti kamerového sledování a přístupu zaměstnavatele k e-mailům zaměstnanců, obsahuje norský zákon pouze zmocnění příslušného ministerstva k vydání bližších pravidel, za kterých lze tato sledování provádět. Tato zmocnění však zatím vydána nebyla. [558] Přesto mají však tamní zaměstnavatelé relativně vysokou míru právní jistoty o tom, jaké způsoby sledování a za jakých podmínek mohou provádět, neboť tamní inspektorát práce jakožto příslušný dozorový orgán vydal detailní a názornou příručku týkající se nutnosti aplikace pravidel ochrany osobních údajů v pracovním prostředí, včetně obsáhlého pojednání o možnostech využívání kontrolních a sledovacích prostředků.[559]

Jsou však také země, kde úroveň regulace je obdobná jako v České republice. Tak je tomu například v Rakousku, Polsku, Nizozemí, Španělsku či Portugalsku, kde obecně není žádný zvláštní předpis či ustanovení týkající se zpracování osobních údajů zaměstnanců či detailněji limitující možnosti sledování a monitoringu zaměstnanců (ve smyslu, že by byly blíže stanoveny podmínky, za kterých lze monitorování provádět atp.). V těchto zemích se

---

[556] Kuschewsky, M. *Data Protection & Privacy, Jurisdictional comparisions.* First edition. London. Sweet & Maxwell, part of Thomson Reuters, 2012, s. 29.

[557] Norwegian Ministry of Labour and Social Affairs. *Act relating to working environment, working hours and employment protection, etc. (Working Environment Act)*. Vydaný dne 1. ledna 2016 [online]. [cit. 2019-05-09]. Dostupný z: https://lovdata.no/dokument/NLE/lov/2005-06-17-62

[558] Osobní konzultace s norskými právními poradci v rámci konference WSG (World Services Group) v Lisabonu, Portugalsko, konané dne 21. a 22. března 2019.

[559] Norwegian Labour Inslection Authority (Arbeidstilsynet). *Guide concerning control and monitoring in working life*. Published: January 2017. [online]. [cit. 2019-05-09]. Dostupné z: https://www.arbeidstilsynet.no/contentassets/04ec2eb566d44942bd6693e9e3a0c99e/guide-concerning-control-and-monitoring-in-working-life_2018.pdf

obvykle vychází z obecných principů, stanovisek lokálních dozorových orgánů či stanovisek WP29.[560]

9.2 De lege ferenda

S ohledem na podaný rozbor v této práci se jako nejpalčivější otázka právní úpravy ochrany osobnosti a osobních údajů zaměstnanců jeví situace, kdy zaměstnavatelé zasahují do soukromí zaměstnanců mimo základní zákonem definovaný rámec, resp. rámec vyplývající z plnění pracovní smlouvy, tedy pokud je právním základem pro zpracování osobních údajů oprávněný zájem zaměstnavatele ve smyslu čl. 6 odst. 1 písm. f) GDPR. Bude se tedy jednat zejména o případy provádění kontrol či monitorování a sledování zaměstnavatelem, které jsou upraveny v § 316 ZPr a jejichž právní regulace je velmi strohá. Na druhou kolej by však neměly být odsouvány ani další otázky, jako je vyžadování a zjišťování si informací od uchazečů o zaměstnání, uchování jejich osobních údajů před, během i po zaměstnání, vyžadování zvláštních kategorií osobních údajů apod. Podle názoru autora této práce by si tyto otázky jistě zasloužily v českém právním řádu větší pozornost. To platí také s ohledem na výše podaný komparativní výklad, který svědčí o tom, že v řadě evropských zemí je této otázce věnována bližší pozornost (byť ne zdaleka ve všech).

Námět, resp. pobídku na legislativní posun lze hledat též v nařízení GDPR, neboť to v čl. 88 přímo vybízí k přijetí pravidel *„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“.*[561] Ve druhém odstavci téhož článku je přitom doplněno, že taková pravidla by se měla vztahovat zejména k *„ochraně lidské důstojnosti, oprávněných zájmů a základních práv subjektů údajů, především pokud jde o transparentnost zpracování, předávání osobních údajů v rámci skupiny podniků nebo uskupení podniků vykonávajících*

[560] Osobní konzultace s vybranými právními poradci z různých evropských zemí v rámci konference WSG (World Services Group) v Lisabonu, Portugalsko, konané dne 21. a 22. března 2019.
[561] Čl. 88 odst. 1 nařízení GDPR. Jak již bylo dříve zmíněno, ustanovení § 316 ZPr nelze podle názoru autora této práce vnímat jako naplnění tohoto ustanovení.

společnou hospodářskou činnost a systémy monitorování na pracovišti".[562] Je zřejmé, že taková pravidla v českém právním řádu schází a jejich přijetí by mohlo odstranit nejistotu a mnoho nejednoznačností, které v současné době panují a se kterými se tato práce snažila vypořádat.

Pro případ využívání různých nástrojů pro monitorování zaměstnanců by podle názoru autora této práce zejména měla existovat jasná pravidla pro konkrétní sledovací prostředky využívané zaměstnavateli, a to alespoň pro kamerové systémy, pro sledování elektronické komunikace a sledování využívání svěřených informačních technologií. Byť by takovým pravidlům bylo možné vyčítat vyšší míru kazuistiky, praxe ukazuje, že jde o velmi závažné otázky, které by měly být regulovány na zákonné úrovni, a nikoliv pouze na základě výkladů podávaných soudy (v lepším případě) či v podobě *soft law* stanovisek a vyjádření různých úřadů a poradních orgánů. Takováto regulace by především měla mít za úkol omezovat využívání těchto prostředků v prostoru (sledování pouze vybraných prostor, kde je zvýšené riziko pro zaměstnavatele, naopak přísný zákaz sledování prostor, kde je očekáváno soukromí, jako šatny apod.) a čase (sledování by mělo být prováděno pouze po omezenou dobu[563]) a měla by jasně definovat možnosti obrany zaměstnanců proti takovýmto nástrojům.[564] Měly by být rovněž blíže vymezeny podmínky informační povinnosti, aby se této povinnosti zaměstnavatel nezprostil jen slovy, že „využívání svěřených prostředků může být monitorováno", ale aby byl zaměstnavatel povinen jasně uvést podmínky takového monitoringu (jaké konkrétní nástroje jsou využívány, jak často apod.).

Kromě monitoringu by větší pozornost zasloužilo též získávání osobních údajů uchazečů o zaměstnání ze sociálních sítí či jinde na internetu a měly by být definovány podmínky, za kterých by zaměstnavatel byl oprávněn takto proaktivně informace o uchazečích získávat. Tyto podmínky by se ostatně mohly vztahovat též na dobu trvání pracovněprávního vztahu, neboť ani po jeho vzniku by zaměstnavatel neměl soukromí zaměstnanců narušovat, nemá-li k opačnému jednání závažné důvody. Nikoliv zbytečnou by bylo též zavedení maximální doby pro uchování údajů uchazeče, neudělí-li k dalšímu zpracování souhlas. Dalšími často diskutovanými otázkami je též využití biometrických

[562] Čl. 88 odst. 2 nařízení GDPR.
[563] Už při nahodilé a občasné kontrole se obvykle dosáhne prakticky shodných výsledků, jako při provádění soustavné kontroly.
[564] Obdobné doporučení na omezení sledování přináší též WP29 (srov. Stanovisko WP29 č. 2/2017: Zpracování údajů na pracovišti (v originále: *opinion 2/2017 on data processing at work).* (WP249), ze dne 8. června 2017, s. 6).

údajů zaměstnanců či informací o zdravotním stavu, tj. bylo by vhodné blíže vymezit, kdy tyto údaje mohou být zaměstnavatelem oprávněně použity a kdy je naopak jejich užití nepřípustné. Názory autora této práce na řešení těchto otázek byly podány výše v příslušných podkapitolách a bodech.

Nabízí se rovněž explicitní zmocnění k vymezení těchto otázek v kolektivních smlouvách. Do budoucna by nemuselo být od věci ani stanovisko k alternativním formám práce (práce z domu, sdílení pracovního prostoru či teleworking), využití geolokačních systémů či chytrých zařízení, případně k situaci, kdy zaměstnanec pro pracovní účely využívá své soukromé prostředky. Z hlediska současné právní úpravy obsažené v § 316 ZPr by bylo též vhodné blíže specifikovat, co se rozumí přiměřeným způsobem kontroly a závažným důvodem spočívajícím ve zvláštní povaze činnosti zaměstnavatele. Samozřejmostí je též již zmiňovaná bližší specifikace rozsahu podávaných informací při sledování zaměstnanců.

Pro potřeby přijetí příslušných pravidel se lze inspirovat nejen ve zmiňovaných zahraničních úpravách, ale také například z již zmiňovaného doporučení Rady Evropy CM/Rec(2015)5.[565] To přitom nabízí nejen obecné doporučení pro nastavení pravidel při zpracování osobních údajů zaměstnanců, ale rovněž doporučení (ve smyslu konkrétních pravidel) pro specifické případy zpracování osobních údajů, jako je monitoring elektronické komunikace, využití IT systémů a kamerových systémů pro sledování zaměstnanců, využití geolokačních zařízení, whistleblowing, zpracování biometrických údajů, psychologické testy atd. Do doby, než bude legislativa upravující výše uvedené otázky schválena, nezbyde než vycházet ze soft law stanovisek dozorových orgánů. Určitou alternativou by ještě mohla být úprava výše uvedených otázek v rámci kolektivních smluv. Tato metoda byla zvolena například v Belgii a je předpokládána též v Německu. U českých kolektivních smluv, alespoň těch vyššího stupně, které jsou veřejně dostupné,[566] se však tyto otázky nezdají být předmětem zájmu. Podle názoru autora této práce však lze očekávat, že se to může brzy změnit, nedojde-li k žádné změně ze strany zákonodárce.

Na národní půdě lze alespoň částečně kladně hodnotit publikaci Ochrana osobních údajů na pracovišti, vydanou v rámci realizace projektu Leonardo da Vinci 2, na které

[565] Op. cit. sub. 35
[566] Ministerstvo práce a sociálních věci České republiky. *Kolektivní smlouvy vyššího stupně uložené na MPSV od 1.1.2007*. [online]. [cit. 2019-05-10]. Dostupné z: https://www.mpsv.cz/cs/3619

ÚOOÚ spolupracoval též s dozorovými orgány z Polska, Bulharska a Chorvatska.[567] Ačkoliv jde částečně o komparativní studii poměřující právní řády všech čtyř zmíněných zemí, lze v ní nalézt odpovědi na většinu klíčových otázek, které si zaměstnavatelé obvykle při potýkání se s ochranou soukromí zaměstnanců kladou. Tomu přispívá i skutečnost, že tato publikace je částečně psaná formou otázek a odpovědí. Publikaci lze označit za velmi přínosnou, jelikož pokrývá celou časovou osu vztahu zaměstnance a zaměstnavatele. Vypořádává se s obsahem životopisu pro dobu před vnikem pracovního poměru, možnostmi dotazů zaměstnavatele na pohovoru, kontaktováním bývalého zaměstnavatele, přípustností souhlasu se zpracováním osobních údajů, hledáním práce na internetu, zapojením agentur práce využitím psychologických testů či online prověřováním uchazeče a pragmaticky radí zaměstnancům či uchazečům, jak si soukromí chránit. Naopak pro dobu trvání pracovního poměru vymezuje publikace vedení pracovního spisu, dobu uchování, předávání osobních údajů, zveřejňování osobních údajů a zpracování zvláštních kategorií osobních údajů. Vedle toho jsou též samozřejmě probrány otázky používání komunikačních prostředků na pracovišti či metody dozoru zaměstnavatele (kamery, biometrické údaje, detektor lži). Samozřejmostí je též popis zpracování osobních údajů po ukončení pracovního poměru.[568]

Bez ohledu na výše uvedené pozitivní aspekty této publikace nejde o příliš propagovaný a mezi zaměstnavateli či zaměstnanci známý dokument. Avšak do doby, než bude přijata odpovídající legislativní úprava, případně dojde k zapracování těchto otázek v rámci kolektivních smluv, by bylo vhodné, aby došlo k aktualizaci tohoto dokumentu, zejména s ohledem na účinnost nařízení GDPR, a zároveň na vztažení výhradně do národního legislativního prostředí (tj. zbavit jej zvláštností aplikovatelných ve třech zbývajících zemích). Ač to není dlouho, co bylo vydáno již několikrát zmiňované stanovisko WP29 týkající se zpracování osobních údajů na pracovišti, to přirozeně nezohledňuje národní specifika, zejména současné ustanovení § 316 ZPr, což by obdobné nařízení vydané ze strany ÚOOÚ dokázalo.

[567] ÚOOÚ: *Ochrana osobních údajů na pracovišti*. Příručka pro zaměstnance. Brno: Masarykova univerzita, 2014.
[568] Tamtéž.

Závěr

Z pohledu ochrany osobnosti i ochrany osobních údajů jakožto samostatných odvětví práva tvoří podmnožina, resp. podmnožiny těchto právních fenoménů týkajících se zaměstnanců relativně samostatné a svébytné soubory právních pravidel. To je způsobeno zejména charakteristickými prvky vztahu mezi zaměstnavatelem a jeho zaměstnanci. Navíc je toto dále umocněno rozvojem informačních technologií, alternativních forem práce a obecně se zlepšujících podmínek práce, které jsou však mnohdy vykoupeny právě zvýšeným zasahováním do soukromí zaměstnanců. U spousty pracovních pozic lze dnes jen stěží hledat hranice mezi domovem a pracovištěm a nevyhnutelně pak dochází k tomu, že do soukromí zaměstnanců není zasahováno jen při práci či na pracovišti, ale též v jejich domácím prostředí.

Ruku v ruce s tím oproti době minulé samozřejmě exponenciálně roste objem zpracovávaných osobních údajů zaměstnanců, a to ve všech ohledech. To se netýká jen možností, jak monitorovat a sledovat zaměstnance, ale obecně správy pracovněprávního vztahu, plnění zákonných povinností apod. Vše lze snadno zálohovat, sdílet či přeposílat, a tak zpracovávané údaje narůstají do obřích rozměrů. Nejcitelnější dopad z hlediska ochrany soukromí mají samozřejmě nejrůznější formy zaznamenávání aktivit zaměstnance. Dříve byly různé systémy či zařízení umožňující skryté sledování doménou bezpečnostních agentur a špionů, dnes si je ale za minimum nákladů může pořídit v podstatě každý a zaměstnavatelům to umožňuje své zaměstnance sledovat a monitorovat na každém kroku. Může jít přitom o systémy či zařízení, o nichž ani zaměstnanci nevědí, resp. nevědí, že mají tuto funkci, přičemž této skutečnosti obvykle nezabrání ani fakt, že zaměstnavatelé musí o jejich existenci informovat (buď z důvodu, že informace je příliš neurčitá, nebo z důvodu, že informace je ukryta někde mezi dalšími desítkami a stovkami povinně poskytovaných informací a zaměstnanci nemají šanci se ve všem zorientovat). Překážkou není ani skutečnost, že údajů o zaměstnancích bývá shromažďováno neúměrně mnoho, neboť opět existují systémy, které si s tím dokážou poradit a za zaměstnavatele udělat práci při analýze získaných údajů.

Ačkoliv technologický vývoj ještě nepochybně není zastaven a je možné očekávat, že tato tendence nárůstu zpracování osobních údajů bude pokračovat, lze s určitou mírou uspokojení konstatovat, že bez ohledu na tento proces je zaměstnancům poskytována dostatečná všeobecná ochrana z hlediska existence a aplikace obecných principů a zásad.

Dokonce je možné pro většinu specifických případů zásahů do jejich soukromí či zpracování jejich osobních údajů vymezit relativně konkrétní právní rámec pro možnost a podmínky takového zasahování ze strany zaměstnavatele. Nutnou podmínkou pro efektivní poskytování ochrany by však bylo, aby též docházelo ke snadnému, rychlému a levnému vymáhání stanovených pravidel. To je otázka, na kterou již tak pozitivně bohužel odpovědět nelze. Ač jde o otázku, která nebyla předmětem zkoumání této práce, je problematika vymahatelnosti práva neoddělitelně spjata s každou právní normou a jen dobře a snadno vymahatelná pravidla dokážou skutečně naplňovat svůj účel. Do určité míry však alespoň může tomuto problému pomoci existence konkrétních specifických norem, tedy takových, které jen minimálně připouští výkladové pochybnosti a za jejichž porušení hrozí vysoké sankce.

Ochrana osobnosti a osobních údajů v pracovněprávních vztazích byla v rámci této disertační práce analyzována z různých hledisek a s různou úrovní detailu, a to s ohledem na v úvodu stanovené dílčí cíle, na které byla v této práci hledána odpověď, resp. kterých byla snaha dosáhnout. V první části práce byly především vyzdvihnuty právní prameny relevantní pro zkoumání této problematiky, což následně posloužilo jako základ pro analýzu prováděnou napříč dalšími částmi celé práce, i když nebyly dále používány veškeré právní předpisy, ale jen ty nejdůležitější z hlediska aplikační použitelnosti, tj. zejména zákony a přímo použitelné předpisy Evropské unie. Zároveň v této první části byla zkoumána a vysvětlena obecná teoretická východiska právních úprav ochrany osobnosti a osobních údajů (bez vazby na pracovněprávní prostředí), jejich jednotlivé prvky, způsoby ochrany a zejména také podobnosti a rozdíly mezi těmito oblastmi práva. Přes různé názory na vztah a prolínání těchto dvou oblastí se autor této práce přiklonil k názoru, že odlišnosti těchto oblastí převažují a je nutné posuzovat a popisovat je odděleně, přestože mnohdy porušení jedné oblasti bude znamenat též porušení druhé (ale ne vždy, jak bylo vysvětleno). Proto je práce strukturována na samostatný výklad týkající se ochrany osobnosti a soukromí zaměstnanců a na samostatný výklad týkající se ochrany osobních údajů.

Ochrana soukromí zaměstnanců a všechny související okolnosti byly důkladně analyzovány ve druhé části této práce. Nadále jsou to zejména vztah nadřízenosti či podřízenosti a určitá závislost zaměstnance na svém zaměstnavateli, co utváří charakter pracovněprávního vztahu. Přestože se právní normy snaží tuto nerovnost a závislost vyvažovat, nelze kazuisticky postihnout veškeré životní situace, které mohou mezi zaměstnancem a zaměstnavatelem nastat. Na druhou stranu ale není vhodná ani situace, kdy

se právní regulace stroze omezuje na využití neurčitých právních pojmů. Proto mají na danou problematiku značný dopad též zkoumaná rozhodnutí soudů a jejich výklad. Nejde jen o rozhodnutí českých soudů, ale také o rozhodnutí jiná, zejména ESLP a tímto soudem dovozený koncept legitimního očekávání soukromí, případně nedávno dovozený koncept, který bez dalšího zakazuje snižovat ochranu soukromí zaměstnance na nulu.

Bylo by také chybou, kdyby ochrana soukromí (jakož i osobních údajů), včetně jejích specifik, byla omezována pouze na trvání pracovněprávního vztahu. Je to zejména situace uchazečů o zaměstnání, která vyžaduje zvláštní pozornost. V tomto ohledu je relativně dobře ošetřen zákaz zaměstnavatele požadovat od zaměstnanců určité informace, na jejichž základě by je mohl nějak znevýhodňovat. Naopak už ale chybí regulace týkající se situací, kdy zaměstnavatel sám proaktivně vyhledává o zaměstnancích určité informace a tím jim zasahuje do soukromí. Extrémním připodobněním by bylo vztažení této situace k relativně mladému trestnému činu nebezpečného pronásledování (tzv. stalkingu), nicméně alespoň rámcové omezení zaměstnavatele v takovémto vyhledávání si informací by si tato otázka do budoucna zasloužila. Ani fázi ukončení pracovněprávního vztahu a následnou ochranu osobnosti zaměstnanců nelze opomíjet. Ačkoliv by se mohlo zdát, že po rozvázání pracovního poměru už nemusí zaměstnance nic trápit ve vztahu k bývalému zaměstnavateli, jsou to zejména černé seznamy (blacklisty), které dokážou zaměstnancům do budoucna značně komplikovat život.

Nepochybně klíčové je však období trvání pracovněprávního vztahu a navazující právo zaměstnance na ochranu jeho soukromí. Není to jen monitoring a sledování činnosti zaměstnanců, kdy je potřeba zaměstnancům zvýšenou ochranu jejich soukromí přiznávat. Jde také o kontrolování zaměstnanců při vnášení svěřených prostředků na pracoviště, případně kontrolování toho, jak zaměstnanci využívají jim svěřené výrobní a pracovní prostředky. Při definování podmínek možnosti sledování zaměstnanců je právní úprava bohužel příliš stručná. Sice umožňuje dovozovat odpovědi na většinu možných otázek, ale cesta k nim je nadměrně složitá, a to i pro osoby znalé práva. Zejména není zřejmý vztah jednotlivých odstavců § 316 ZPr, začlenění čtvrtého odstavce je zcela nesystematické, jsou použity značně neurčité právní pojmy, nejsou definovány podmínky plnění informační povinnosti apod. Tyto nedostatky rozhodně vymahatelnosti ochrany soukromí pro zaměstnance nepřispívají.

Dalo by se říci, že problematika ochrany osobních údajů zaměstnanců, která byla analyzována v rámci třetí části této práce, je zcela odlišná, neboť je relativně komplexní

a obsáhlou právní úpravou. Nařízením GDPR upravená pravidla se sice netýkají zpracování osobních údajů zaměstnanců, neboť jde o obecná pravidla, ale jejich vztažení na zpracování osobních údajů prováděné zaměstnavatelem nečiní větší obtíže. Určité potíže se nicméně mohou vyskytovat při aplikaci těchto norem v praxi, která nemusí být vždy zcela snadná a jednoznačná. To platí dokonce pro odbornou právnickou veřejnost, která ne vždy má s uplatňováním pravidel ochrany osobních údajů větší zkušenosti. Jako příklad lze uvést nadužívání souhlasů se zpracováním osobních údajů (zejména u zaměstnanců). Ale ani mezi zasvěcenějšími osobami nepanuje vždy jasná shoda o tom, jaký právní základ je možné aplikovat na které operace zpracování osobních údajů. Obdobně ne vždy je zcela jasné, jaké činnosti lze definovat ještě jako zpracování osobních údajů a co už je mimo rámec této regulace.

Kromě toho existuje také celá řada obecně vyjádřených povinností, jejichž splnění může být pro zaměstnavatele velmi obtížné, či dokonce nemožné. Jde například o povinnosti související s minimalizací osobních údajů, omezením doby jejich uložení, zpracováním zvláštních kategorií osobních údajů, důsledným naplněním některých práv (právo získat kopie všech zpracovávaných osobních údajů), sdílením osobních údajů zaměstnanců se třetími stranami apod. Nehledě na celou řadu povinností, které jsou zaměstnavatelům uloženy nad rámec přímého vztahu se zaměstnancem, jako je vedení záznamů o činnostech, zajišťování odpovídajícího zabezpečení osobních údajů či provádění posouzení vlivu na ochranu osobních údajů. Je proto možné dojít k závěru, že těchto povinností je na zaměstnavatele stanoveno až příliš. Na druhou stranu je podle názoru autora této práce z hlediska poskytování ochrany lepší variantou, pokud je pravidel více a dochází k naplňování alespoň některých z nich, než když je pravidel sice málo, ale jsou nesrozumitelná či neurčitá, a proto k jejich naplňování nedochází vůbec, jen minimálně či se značnými obtížemi.

Záměrem závěrečné čtvrté části bylo zaměřit se na vybrané aplikační otázky z hlediska ochrany soukromí i osobních údajů (zejména na způsoby monitoringu a sledování zaměstnanců), nahlédnout do zahraničních právních úprav, poskytnout určité shrnutí a zamyslet se nad tím, jakým způsobem by se příslušná právní úprava mohla ubírat do budoucna. Praxe již delší dobu potvrzuje, že existuje relativně omezený okruh nejčastěji využívaných způsobů monitoringu a sledování zaměstnanců. Aplikace principů ochrany soukromí a právních pravidel obsažených v ZPr přitom vždy neposkytuje zcela jasné odpovědi a ani není snadná. Příklady ze zahraničí přitom jasně ukazují, že lze tyto způsoby

(resp. alespoň některé z nich) právně blíže formulovat a definovat podmínky, za kterých mohou být využity. Na druhou stranu nelze říci, že by česká právní úprava byla svým přístupem k této otázce nějak výrazně za průměrem, neboť v řadě zkoumaných zemí je situace velmi podobná situaci v České republice.

I přesto se autor této práce domnívá, že současný stav je třeba řešit. Ochrana poskytovaná zaměstnancům v rámci ZPr není dostatečná a mělo by dojít k důslednému naplnění legislativního zmocnění obsaženého v čl. 88 GDPR. Je nutné si totiž uvědomit, že ochranná funkce pracovního práva je z tohoto hlediska současným vývojem postupně omezována. Ustanovení § 316 ZPr v době svého vzniku mělo jiné aplikační dopady a jiné dopady má dnes. Co bylo dříve považováno za výjimečné opatření, ať už jde o využití kamerových systémů, nebo nástrojů pro sledování práce s počítačem, je dnes považováno za běžnou součást našich životů. To má samozřejmě ten neblahý důsledek, že využití takovýchto nástrojů bývá ze strany zaměstnavatelů považováno za samozřejmé a v praxi je, i s ohledem na nižší pořizovací náklady, velmi rozšířené. Zaměstnavatelé se mnohdy brání, že uvedené monitorování a sledování určitých oblastí (zejména prostřednictvím kamer) je prováděno výhradně kvůli zákazníkům či obchodním partnerům. Jakmile se však na záznamu objevují zaměstnanci, nemůže a nemělo by být toto tvrzení považováno za relevantní. Nikdo kromě samotného zaměstnavatele totiž nedokáže v dané situaci s jistotou prokázat či zaručit, že pořízené záznamy nebudou využity i proti zaměstnanci. Přesně v takovém případě by se měla projevit ochranná funkce pracovního práva, která by tuto činnost zaměstnavateli zakázala či omezila.

Výše nastíněný vývoj však nelze bez dalšího přecházet a je třeba s ním bojovat. Právě s ohledem na tyto závěry by měla být zmiňovaná ochranná funkce pracovního práva v tomto případě posílena. Takové pracovní prostředí, kde jsou zaměstnanci při veškerých činnostech sledováni, je v konečném důsledku vystavuje neúměrnému tlaku a může mít paradoxně negativní důsledky z hlediska jejich výkonnosti, bezpečnosti práce, ale i sociálního života a vztahů na pracovišti (o tomto tématu sice práce nepojednává, ale nepochybně si i tato otázka zaslouží pozornost a určitou ochranu). Právní ochrana obsažená v ustanovení § 316 ZPr se sice může jevit z obecného hlediska i nadále dostatečná, neboť by veškeré moderní výdobytky měla postihovat, přesto je to však právě stručnost této právní úpravy a její relativně nízká vymahatelnost (nemluvě o skutečnosti, že je to relativně krátce, co lze přímo postihovat porušování ustanovení § 316 ZPr), která ochranu soukromí v dnešní době značně omezuje. O nízké vymahatelnosti koneckonců svědčí i nízký počet českých soudních

rozhodnutí, která se této otázce věnují. Větší a snazší vymahatelnosti zaměstnanci obvykle dosáhnou, pokud se se svou stížností obrátí na dozorové orgány, jako je ÚOOÚ či inspektorát práce. Soudní ochrana je pro ně jednoduše příliš komplikovaná. Protože ale změna v této otázce vymahatelnosti je otázkou systémovou, kterou nelze řešit jednoduše změnou několika málo právních ustanovení, nabízí se dle autora této práce částečné řešení, které již bylo nabídnuto, a tím je bližší regulace specifických monitorovacích nástrojů využívaných ze strany zaměstnavatelů.

Seznam zkratek

BOZP	Bezpečnost a ochrana zdraví při práci
ESLP	Evropský soud pro lidská práva
EÚLP	Evropská úmluva o ochraně lidských právech
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, obecné nařízení o ochraně osobních údajů
LZPAS	Listina základních práv a svobod
LZPEU	Listina základních práva Evropské unie
MOP	Mezinárodní organizace práce
MPOPP	Mezinárodní pakt o občanských a politických právech
OSN	Organizace spojených národů
ObčZ	Zákon č. 89/2012 Sb., občanský zákoník
WP29	Pracovní skupina zřízená na základě čl. 29 Směrnice (anglicky *Article 29 Data Protection Working Party*)
SDEU	Soudní dvůr Evropské unie
SFEU	Smlouva o fungování Evropské unie
Směrnice	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
PřesZ	Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich
TOPO	Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
ÚOOÚ	Úřad pro ochranu osobních údajů
Úmluva 108	Úmluva č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat
VDLP	Všeobecná deklarace lidských práv
ZoIP	Zákon č. 251/2005 Sb., o inspekci práce
ZOOÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném do 23. dubna 2019
ZoZ	Zákon č. 435/2004 Sb., o zaměstnanosti
ZZOÚ	Zákon č. 110/2019 Sb., o zpracování osobních údajů
ZPr	Zákon č. 262/2006 Sb., zákoník práce

Seznam použitých zdrojů

Seznam použité literatury

BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: vybrané problémy*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. ISBN 978-80-7552-141-5.

BARTÍK, Václav a Eva JANEČKOVÁ. Zákon o ochraně osobních údajů s komentářem. Olomouc: ANAG, 2010. Právo. ISBN 978-80-7263-613-6.

BARTOŇ, Michal, Jan KRATOCHVÍL, Martin KOPA, Maxim TOMOSZEK, Jiří JIRÁSEK a Ondřej SVAČEK. *Základní práva*. Praha: Leges, 2016. Student. ISBN 978-80-7502-128-1.

BĚLINA, Miroslav. *Zákoník práce: komentář*. 2. vyd. Praha: C.H. Beck, 2015. Velké komentáře. ISBN 978-80-7400-290-8.

BĚLINA, Miroslav, Jan PICHRT, Petr HŮRKA, Jakub MORÁVEK, Věra ŠTANGOVÁ, Martin ŠTEFKO, Petr TRÖSTER a Margerita VYSOKAJOVÁ. Pracovní právo. 7. doplněné a podstatatně přepracované vydání 2017. Praha: C.H. Beck, 2017. Academia iuris. ISBN 978-80-7400-667-8.

HARRIS, D. J., M. O'BOYLE, Ed BATES, et al. Harris, O'Boyle & Warbrick: *Law of the European Convention on Human Rights*. Third edition. Oxford, United Kingdom: Oxford University Press, 2014. ISBN 978-0-19-960639-9.

HENDRYCH, Dušan a kol. *Právnický slovník*. 3. podstatně rozšířené vydání. Praha: C. H. Beck, 2009, 1481 s., ISBN 978-80-7400-059-1.

JANEČKOVÁ, Eva a Václav BARTÍK. Ochrana osobních údajů v pracovním právu: (otázky a odpovědi). Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3.

JANEČKOVÁ, Eva a Václav BARTÍK. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde Praha, 2011. Praktická právnická příručka. ISBN 978-80-7201-850-5.

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

KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0.

KUSCHEWSKY, Monika. *Data Protection & Privacy, Jurisdictional comparisions*. First edition. London. Sweet & Maxwell, part of Thomson Reuters, 2012. ISBN: 978-1-908239-14-3.

LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. Komentář. 1. vydání, Praha: C. H. Beck, 2014, 2400 s., ISBN 978-80-7400-529-9.

MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. *Ochrana osobních údajů*. Praha: Leges, 2012. Praktik. ISBN 978-80-87576-12-0.

MELZER, Filip. *Občanský zákoník: velký komentář*. Svazek I. § 1-117. 1. vyd. Praha: Leges, 2013. Komentátor. ISBN 978-80-87576-73-1.

MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013. Právní rukověť. ISBN 978-80-7478-139-1.

NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohuslav, TOMÍŠEK, Jan. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

PICHRT, Jan. *Zákoník práce: Zákon o kolektivním vyjednávání*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-609-0.

POMAHAČ, Richard a Lenka PÍTROVÁ. *Průvodce judikaturou Evropského soudního dvora*. Díl 1. Praha: Linde, 2000. ISBN 80-7201-204-5.

SOLOVE, Daniel J., SCHWARTZ, Paul M. *Privacy Law Fundamentals*. Portsmouth: International Association of Privacy Professionals, 2017. ISBN 978-0-9983223-1-5.

ŠÁMAL, Pavel. *Trestní odpovědnost právnických osob: komentář*. 2. vydání. V Praze: C.H. Beck, 2018. Beckova edice komentované zákony. ISBN 978-80-7400-592-3.

ŠIMÍČEK, Vojtěch (ed.). Právo na soukromí. 1. vyd. Brno: Masarykova univerzita, 2011. ISBN 978-80-210-5449-3.

TICHÝ, Luboš. *Obecná část občanského práva*. V Praze: C.H. Beck, 2014. Právní praxe. ISBN 978-80-7400-483-4.

TOMÁŠEK, Michal, TÝČ, Vladimír a kol. *Právo Evropské unie*. 2. aktualizované vydání. Praha: Leges, 2017, 496 s., ISBN 978-80-7502-184-7.

TRÖSTER, Petr. *Právo sociálního zabezpečení*. 6. podstatně přepracované a aktualizované vydání. Praha: C. H. Beck, 2013. Academia iuris. ISBN 978-80-7400-473-5.

ÚOOÚ: *Ochrana osobních údajů na pracovišti*. Příručka pro zaměstnance. Brno: Masarykova univerzita, 2014, 36 s. ISBN 978-80-210-6819-3.

VIDRNA, Jan a Zdeněk KOUDELKA. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců*. V Praze: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7.

WEIR, Robert E. *Workers in America: a historical encyclopedia*. Vol. 1. Santa Barbara, California. ABC-CLIO, LLC, 2013. ISBN 978-1-59884-718-5.

Seznam časopiseckých článků

FETTER, Richard W. *Pracovní posudek*. Právní rádce. 2010, č. 8, 21-22. ISSN 1210-4817.

FIALOVÁ, Eva. *Ochrana soukromí ve světle judikatury Evropského soudu pro lidská práva*. Časopis pro právní vědu a praxi. 2012, roč. 20, č. 2, 121-127. ISSN 1210-9126

HŮRKA, P. *Změny v pracovním právu v souvislosti s novým občanským zákoníkem*. Právní rozhledy. 2014, 22 (7), 233-240. ISSN 1210-6410.

JOUZA, Ladislav. *Ochrana osobnosti zaměstnance v pracovněprávních vztazích*. Bulletin advokacie. 2014, č. 6, 26-30. ISSN 1210-6348.

LANDWEHRMANN, Tereza. *Kontrola vnášených a vynášených věcí na pracovišti*. Praktická personalistika. 2016, č. 7-8. ISSN 2336-5072.

MATES, Pavel. *Nad některými oblastmi nového zákona o odpovědnosti za přestupky a řízení o nich.* Bulletin advokacie. 2016. č. 12, 25-30. ISSN 1210-6348.

MORÁVEK, Jakub. *Kontrola a sledování zaměstnanců – výklad § 316 ZPr*. Právní rozhledy. 2017. 25 (17), 573-581. ISSN 1210-6410.

MORÁVEK, Jakub. *Sledování zaměstnanců v kontextu novely zákoníku práce*. Právní rozhledy. 2012, 20 (5), 175-181. ISSN 1210-6410.

NONNEMANN, František. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. Právní rozhledy. 2012, 20(13), 505-509. ISSN 1210-6410.

NONEMANN, František. *Soukromí na pracovišti*. Právní rozhledy. 2015, 23 (7), 229-237. ISSN 1210-6410.

PICHRT, Jan, MORÁVEK, Jakub. *Whistleblowing*. Právo pro podnikání a zaměstnání. 2009, 18(7-8), 19-25. ISSN 1801-6014.

PICHRT, Jan. *Alternativní řešení pracovněprávních sporů – strašák současnosti či naděje budoucnosti?* Sborník příspěvků z mezinárodní konference Pracovní právo 2016 na téma Zákoník práce v novelizaci, důchodová reforma v akci. Masarykova Univerzita, 2017. ISBN 978-80-210-8528-2.

RADIČOVÁ, Zuzana. *Monitoring zaměstnanců prostřednictvím GPS technologie.* Právní rozhledy. 2014. 22(21), 736-740. ISSN 1210-6410.

SUDER, Seili. *Pre-employment Background Checks on Social Networking Sites - may your boss be watching?* Masaryk University Journal of Law and Technology, 2014, Vol. 8:1, 123-136. ISSN 1802-5943.

SELTENREICH, Radim. *Právo na soukromí v kontextu ústavního vývoje USA*. Právník. 2000, 139(1), 23-26. ISSN 0231-6625.

ŠTEFKO, Martin. *Ochrana soukromí zaměstnanců ve světle čl. 8 Úmluvy o ochraně lidských práv a základních svobod*. Jurisprudence. 2012, č. 7-8, 17-22. ISSN 1802-3843.

ŠTĚDROŇ, Bohumír. *Čtení e-mailové pošty zaměstnavatelem a ochrana soukromí*. Bulletin advokacie. 2004. č. 10, 48-51. ISSN 1210-6348.

ŠVAŇHAL, Roman. *Ochrana osobnosti fyzický osob*. Právní rozhledy. 2000, 9, s. 385. ISSN 1210-6410.

TELEC, Ivo. *Přirozené právo osobnostní a jeho státní ochrana*. Právní rozhledy. 2007, 15(1), 1-10. ISSN 1210-6410.

TELEC, Ivo. *Chráněné statky osobnostní*. Právní rozhledy. 2007, 15(8), 271-281. ISSN 1210-6410.

VROMAN, Margaret, STULZ, Karin, HART, Claudia, STULZ, Emily. *Employer Liability for Using Social Media in Hiring Decisions*. Journal Social Media for Organizations, 2016, Vol. 3, Issue 1. 1-12. ISSN 2471-8351.

WARREN Samuel D., BRANDEIS Louis D. *The Right to Privacy*. Harvard Law Review. 1890, Vol. 4, No. 5., 193-220. ISSN 0017-811X.

ZAHRADNÍČEK, Jaroslav. *Sledování elektronických komunikací na pracovišti.* Právní rádce. 2016, 50-55. ISSN 1210-4817.

Seznam použitých internetových zdrojů

Act on the Protection of Privacy in Working Life (759/2004). © Ministry of Labour, Finland. [online]. [cit. 2019-05-08]. Dostupné z: https://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf.

BARTOŠ, Vojtěch. *Právo být zapomenut? Spíše právo na rozmazané vzpomínky…* Jiné právo. Publikováno dne 31. května 2014 [online]. [cit. 2019-04-30]. Dostupné z: http://jinepravo.blogspot.com/2014/05/vojtech-bartos-pravo-byt-zapomenut-spis.html.

Belgium Data Protection Authority: *Modèle de Registre des activités de traitement.* Published August 2017 [online]. [cit. 2019-04-17]. Dostupné z: https://www.autoriteprotectiondonnees.be/canevas-de-registre-des-activites-de-traitement.

BLOCK, Richard N., BERG, Peter, BELMAN, Dale. *The Economic Dimension of the Employment Relationship*. in *The Employment Relationship:Examining Psychological and Contextual Perspectives*. Oxford: Oxford University Press, 2004, 94-118 [online]. [cit. 2019-01-05]. Dostupné z: https://msu.edu/~block/documents/Coyle-ch05RBChangesJan2304.pdf.

Bundesdatenschutzgesetz (BDSG) z 30. června 2017 (BGBl. I S. 2097) [online]. [cit. 2019-05-08]. Dostupný z: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0222.

Can Social Media Get You Fired, Elizabeth Garone in BBC Capital, 3. listopadu 2014 [online]. [cit. 2018-11-05]. Dostupné z: http://www.bbc.com/capital/story/20130626-can-social-media-get-you-fired.

CARMONA, Magdalena Sepúlveda. *Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection*. ESS - Working paper No. 59. International Labour Office (ILO). 5 června 2018. 70 s., ISSN 1020-959X. [online]. [cit. 2018-11-05]. Dostupné z: https://harvardlpr.com/wp-content/uploads/sites/20/2016/06/10.2_7_Rogers.pdf.

Commission Nationale de l'Informatique et des Libertés (CNIL): *Le registre des activités de traitement*. [online]. [cit. 2019-04-17]. Dostupné z: https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement.

Datenschutzstelle Fürstentum Liechtenstein: *Verzeichnis Verarbeitungstätigkeiten (Art. 30 DSGVO)*. [online]. [cit. 2019-01-17]. Dostupné z: https://www.datenschutzstelle.li/datenschutz/themen-z/verzeichnis-verarbeitungstaetigkeiten.

DAVISON, Kristl H., MARAIST, Catherine. C., HAMILTON, R. H., BING, Mark N. *To Screen or Not to Screen? Using the Internet for Selection Decisions*. Employee Responsibilities and Rights Journal, 2012, vol. 24, no. 1. [online]. [cit. 2019-02-05]. Dostupné z: https://www.academia.edu/10086027/To_Screen_or_Not_to_Screen_Using_the_Internet_for_Selection_Decisions.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern: *Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz*. Januar 2016 [online]. [cit. 2019-04-30]. Dostupné z:

https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Broschueren/oh-internet-arbeitsplatz.pdf.

Doporučení Rady Evropy č. CM/Rec(2015)5 týkající se zpracování osobních údajů na pracovišti, ze dne 1. dubna 2015 [online]. [cit. 2018-11-10]. Dostupné z: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a.

Doporučení Rady Evropy č. R (89) 2, o ochraně osobních údajů využívaných pro potřeby zaměstnání, ze dne 18. ledna 1989 [online]. [cit. 2018-11-10]. Dostupné z: https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf.

Endorsement of GDPR WP29 guidelines by the EDPB. In edpb.europa.eu, 25. května 2018 [online]. [cit. 2018-11-15]. Dostupné z: https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_cs.

French prosecutors push for Ikea trial over spying charges. In The Local.se, 11. ledna 2018 [online]. [cit. 2018-11-05]. Dostupné z: https://www.thelocal.se/20180111/french-prosecutors-push-for-ikea-trial-over-spying-charges.

HROMADA, Miroslav. Ochrana osobnosti zaměstnanců v soudní praxi. In Pracovní právo 2017, sborník na téma Ochrana osobních údajů, služební zákon a sociální souvislosti zaměstnávání cizinců [online]. [cit. 2018-12-10]. Dostupné z: https://www.law.muni.cz/sborniky/pracpravo2017/files/008.html.

Information Commissioner's Office (ICO): How do we document our processing activities? [online]. [cit. 2019-04-17]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/.

International Labour Office (ILO). Code of Pracite: Protection of workers' personal data. Geneva, International Labour Office, 1997. ISBN 92-2-110329-3. [online]. [cit. 2019-04-19]. Dostupný z: https://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf.

KENNEDY, Nicole, MACKO, Matt. *Social Networking Privacy and Its Effects on Employment Opportunities*. The information age, 2, 111–23. 2009. [online]. [cit. 2019-02-06]. Dostupné z: http://www.ethicapublishing.com/inconvenientorinvasive/2CH12.pdf.

Kodex Severní Karoliny, Kapitola 14 Trestní právo. Článek 45 – Regulace zaměstnavatele a zaměstnance. 14-355. Blacklisting employees (cit. NC Gen Stat § 14-355) [online]. [cit. 2019-02-11]. Dostupný z: https://www.labor.nc.gov/workplace-rights/employee-rights-regarding-time-worked-and-wages-earned/job-reference-and-0.

Ministerstvo práce a sociálních věci České republiky. *Kolektivní smlouvy vyššího stupně uložené na MPSV od 1.1.2007*. [online]. [cit. 2019-05-10]. Dostupné z: https://www.mpsv.cz/cs/3619.

Ministerstvo vnitra České republiky: *Vzorové dokumenty*. Metodická podpora a konzultace [online]. [cit. 2019-04-17]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/vzorove-dokumenty.aspx?q=cHJuPTE%3d.

MRÁZ, Miroslav. *Bezúhonnost v právním řádu České republiky*. © EPRAVO.CZ. Publikováno dne 1. prosince 2015 [online]. [cit. 2019-04-02]. Dostupné z:

https://www.epravo.cz/top/clanky/bezuhonnost-v-pravnim-radu-ceske-republiky-99570.html.

Návrh zákona o ochraně oznamovatelů. Předkladatel: Ministerstvo spravedlnosti, č. j. OVA 140/19. Elektronická knihovna připravované legislativy pro veřejnost [online]. [cit. 2019-05-06]. Dostupné z: https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=3&_material_WAR_odokkpl_pid=ALBSB9HFJX37&tab=detail.

NONNEMANN, František. Modernizace Úmluvy 108, základního nástroje Rady Evropy pro ochranu osobních údajů. In epravo.cz. 20 července 2018. [online]. [cit. 2019-01-11]. Dostupné z: https://www.epravo.cz/top/clanky/modernizace-umluvy-108-zakladniho-nastroje-rady-evropy-pro-ochranu-osobnich-udaju-107901.html.

NONNEMANN, František. *Privacy by design jako jedno z nových pravidel pro zpracování osobních údajů?* © EPRAVO.CZ. Publikováno dne 20. dubna 2018. [online]. [cit. 2019-03-02]. Dostupné z: https://www.epravo.cz/top/clanky/privacy-by-design-jako-jedno-z-novych-pravidel-pro-zpracovani-osobnich-udaju-107367.html.

Norwegian Labour Inslection Authority (Arbeidstilsynet). *Guide concerning control and monitoring in working life*. Published: January 2017. [online]. [cit. 2019-05-09]. Dostupné z: https://www.arbeidstilsynet.no/contentassets/04ec2eb566d44942bd6693e9e3a0c99e/guide-concerning-control-and-monitoring-in-working-life_2018.pdf.

Norwegian Ministry of Labour and Social Affairs. *Act relating to working environment, working hours and employment protection, etc. (Working Environment Act)*. Vydaný dne 1. ledna 2016 [online]. [cit. 2019-05-09]. Dostupný z: https://lovdata.no/dokument/NLE/lov/2005-06-17-62.

PERRY, Nick. *Indecent Exposures: Theorizing Whistleblowing*. Department of Sociology. The University of Auckland, New Zealand, Volume: 19 issue: 2, page(s): 235-257, Publikováno 1. března 1998 [online]. [cit. 2018-05-04]. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.923.9031&rep=rep1&type=pdf.

Rada Evropy: 28 January – Data protection day. In coe.int. 28 ledna 2019 [online]. [cit. 2019-02-01]. Dostupné z: https://www.coe.int/bs/web/portal/28-january-data-protection-day.

Revelations That Ikea Spied on Its Employees Stir Outrage in France. In The New York Times, 15. prosince 2013 [online]. [cit. 2018-11-05]. Dostupné z: https://www.nytimes.com/2013/12/16/business/international/ikea-employee-spying-case-casts-spotlight-on-privacy-issues-in-france.html.

ROGERS, Brishen. *Employment Rights in the Platform Economy: Getting Back to Basics*. Harvard Law & Policy Review, vol. 10, 2016 [online]. [cit. 2019-02-01]. Dostupné z: https://harvardlpr.com/wp-content/uploads/sites/20/2016/06/10.2_7_Rogers.pdf.

SANDERS, Sherry Denise. *Privacy is Dead: The Birth of Social Media Background Checks*. Southern University Law Center REV. 24, 2012 [online]. [cit. 2019-02-05]. Dostupné z: https://ssrn.com/abstract=2020790.

Sborník Dolní Komory Spojeného království: House of Commons, Scottish Affairs Committee. *Blacklisting in Employment. Oral and written evidence*. Publikováno 16. dubna 2013 [online]. [cit. 2019-02-10]. Dostupné z: https://publications.parliament.uk/pa/cm201213/cmselect/cmscotaf/156/156i.pdf.

Státní úřad inspekce práce. *Monitorování zaměstnanců na pracovišti kamerovým systémem*. Otázky a odpovědi. Přidáno dne 7. dubna 2014 [online]. [cit. 2019-02-27]. Dostupné z: http://www.suip.cz/otazky-a-odpovedi/pracovnepravni-vztahy/ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance/monitorovani-zamestnancu-na-pracovisti-kamerovym-systemem-pridano-7-4-2014/.

STEINBOCK, Daniel J. *Designating the Dangerous: From Blacklists to Watch Lists*. Seattle University Law Review, Vol. 30:65, 2006 [online]. [cit. 2019-02-05]. Dostupné z: https://ssrn.com/abstract=905299.

The Council of Europe at 70: Milestones and achievements. In coe.int. 2 května 2019 [online]. [cit. 2019-05-07]. Dostupné z: https://www.coe.int/en/web/secretary-general/-/the-council-of-europe-at-70-milestones-and-achievements.

ÚOOÚ: GDPR (obecné nařízení). *K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů.* Publikováno dne 8. února 2019 [online]. [cit. 2019-04-21]. Dostupné z: https://www.uoou.cz/k-povinnosti-spravcu-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/ds-5458/archiv=0&p1=3938.

ÚOOÚ: GDPR (obecné nařízení). *Zpracovatel* [online]. [cit. 2019-04-17]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=33194&n=k-povinnosti-spravcu-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju.

ÚOOÚ: Poradna. *Jaké informace by měl obsahovat záznam o činnostech zpracování pro nejmenší podnikatele?* [online]. [cit. 2019-04-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30185.

ÚOOÚ: *Rubrika Právní předpisy*. In uoou.cz [online]. [cit. 2018-11-16]. Dostupné z: https://www.uoou.cz/pravni-predpisy/ds-1257/p1=1257.

ÚOOÚ: Sekce: často kladené dotazy. *Ke kamerám a kamerovým systémům* [online]. [cit. 2019-04-17]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5041&n=ke-kameram-a-kamerovym-systemum.

ÚOOÚ: Sekce: často kladené dotazy. *Zaměstnavatelé* [online]. [cit. 2019-04-15]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5057&n=zamestnavatele.

ÚOOÚ: Sekce: často kladené dotazy. *K vyžadování souhlasu* [online]. [cit. 2019-03-11]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5047&n=k-vyzadovani-souhlasu.

ÚOOÚ: *Ke zpracování osobních údajů bývalých zaměstnanců*. Závěry z rozhodnutí ÚOOÚ sp. zn. č. j. SKO-2077/07. Vytvořeno dne 21. března 2013 [online]. [cit. 2019-03-25]. Dostupné z: https://www.uoou.cz/ke-zpracovani-osobnich-udaju-byvalych-zamestnancu/d-1585/p1=1279.

ÚOOÚ: Výsledky dotazníkového průzkumu mezi účastníky seminářů pro pověřence pro ochranu osobních údajů v říjnu 2018. Publikovaná dne 31. října 2018 [online]. [cit. 2019-03-20]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32270.

ÚOOÚ: Tisková zpráva. *Sdělení předsedkyně Úřadu k vyžadování souhlasu*. Publikováno dne 31. srpna 2018 [online]. [cit. 2019-03-08]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31695.

ÚOOÚ: Tisková zpráva. *Poznatky Úřadu k používání G*DPR. Publikováno dne 9. listopadu 2018 [online]. [cit. 2019-03-08]. Dostupné z: https://www.uoou.cz/poznatky-uradu-k-nbsp-pouzivani-gdpr/d-32252.

VYMĚTAL, Petr. *Černé listiny*. Pracovní text pro Ministerstvo vnitra ČR. Katedra politologie, fakulta mezinárodních vztahů, Vysoká škola ekonomická v Praze [online]. [cit. 2019-02-10]. Dostupné z: https://www.mvcr.cz/soubor/studie-vymetal-blacklisting-pdf.aspx.

WINN, Peter A. *Katz and the Origins of the „Reasonable Expectation of Privacy" Test*. McGeorge Law Review, Forthcoming, Vol. 40, Issue 1, 2009 [online]. [cit. 2019-02-03]. Dostupné z: https://ssrn.com/abstract=1291870.

YANIKY-RAVID, Shlomit. *To Read Or Not to Read: Privacy within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory*. American University Law Review, Vol. 64, No. 1, [online]. [cit. 2019-02-01]. Dostupné z: https://ssrn.com/abstract=2231694.

Seznam použitých právních předpisů

Smlouva o fungování Evropské unie

Všeobecná deklarace lidských práv

Listina základních práv Evropské unie

Úmluva č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat.

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

Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů

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

Zákon č. 170/2018 Sb., o distribuci pojištění a zajištění

Zákon č. 251/2016 Sb., o některých přestupcích, ve znění pozdějších předpisů

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

Zákon č. 234/2014 Sb., o státní službě, ve znění pozdějších předpisů

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

Zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů

Zákon č. 373/2011 Sb., o specifických zdravotních službách, ve znění pozdějších předpisů

Zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů

Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon), ve znění pozdějších předpisů

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

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů

Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

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

Zákon č. 412/2005 Sb., o ochraně utajovaných informací, ve znění pozdějších předpisů

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

Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů

Zákon č. 435/2004 sb., zákon o zaměstnanosti, ve znění pozdějších předpisů

Zákon č. 361/2003 Sb. o služebním poměru příslušníků bezpečnostních sborů, ve znění pozdějších předpisů

Zákon č. 231/2001 Sb., zákon o rozhlasovém a televizním vysílání, ve znění pozdějších předpisů

Zákon č. 120/2001 Sb., exekuční řád, ve znění pozdějších předpisů

Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů

Zákon č. 118/2000 Sb., o ochraně zaměstnanců při platební neschopnosti zaměstnavatele a o změně některých zákonů, ve znění pozdějších předpisů

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném do 23. dubna 2019

Zákon č. 46/2000 Sb., tiskový zákon, ve znění pozdějších předpisů

Zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů

Zákon č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů

Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů

Zákon č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění, ve znění pozdějších předpisů

Zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení, ve znění pozdějších předpisů

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

Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů

Zákon č. 582/1991 Sb. o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů

Zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů

Zákon č. 451/1991 Sb., kterým se stanoví některé další předpoklady pro výkon některých funkcí ve státních orgánech a organizacích České a Slovenské Federativní Republiky, České republiky a Slovenské republiky, ve znění pozdějších předpisů.

Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů

Nařízení vlády č. 145/2015 Sb. o opatřeních souvisejících s oznamováním podezření ze spáchání protiprávního jednání ve služebním úřadu

Nařízení vlády č. 201/2010 Sb., o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu, ve znění pozdějších předpisů

Nařízení vlády č. 361/2007 Sb., kterým se stanoví podmínky ochrany zdraví při práci

Vyhláška č. 361/2016 Sb. o zabezpečení jaderného zařízení a jaderného materiálu, ve znění pozdějších předpisů

Vyhláška č. 225/2015 Sb. o stanovení rozsahu bezpečnostních opatření fyzické ochrany objektu zařazeného do skupiny A nebo skupiny B, ve znění pozdějších předpisů

Vyhláška č. 163/2014 Sb. o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry, ve znění pozdějších předpisů

Vyhláška č. 125/1993 Sb. o zákonném pojištění odpovědnosti zaměstnavatele za škodu při pracovním úrazu nebo nemoci z povolání, ve znění pozdějších předpisů

Evropská úmluva o lidských právech (sdělení č. 209/1992 Sb.)

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

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

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 o soukromí a elektronických komunikacích)

Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES

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

Seznam použité judikatury

Rozhodnutí Nejvyššího soudu ČR ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011

Rozhodnutí Nejvyššího soudu ČR ze dne 7. srpna 2014, sp. zn. 21 Cdo 747/2013
Rozhodnutí Nejvyššího soudu ČR ze dne 22. dubna 2003, sp. zn. 21 Cdo 1893/2002
Rozhodnutí Nejvyššího soudu ČR ze dne 17. května 2005, sp. zn. 21 Cdo 2152/2004
Rozhodnutí Nejvyššího soud ČR ze dne 18. července 2013, sp zn. 21 Cdo 1362/2012
Rozhodnutí Nejvyššího soudu ČR ze dne 20. března 2017, sp. zn. 21 Cdo 1043/2016
Rozhodnutí Nejvyššího soudu ČR ze dne 4. dubna 2017, sp. zn. 21 Cdo 3998/2016
Rozhodnutí Nejvyššího soudu ČR ze dne 21. března 2013, sp. zn. 21 Cdo 560/2012
Rozhodnutí Nejvyššího soudu ČR ze dne 21. ledna 2014, sp. zn. 21 Cdo 1496/2013
Rozhodnutí Nejvyššího soudu ČR ze dne 7. června 2017, sp. zn. 21 Cdo 817/2017
Nález Ústavního soudu ČR ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10
Nález Ústavního soudu ČR ze dne 6. března 2012, sp. zn. Pl. ÚS 1586/09
Nález Ústavního soudu ČR ze dne 1. března 2000, sp. zn. II. ÚS 517/99
Nález Ústavního soudu ČR ze dne 7. dubna 2010, sp. zn. I. ÚS 22/10
Nález Ústavního soudu ČR ze dne 12. března 2008, sp. zn. Pl. ÚS 83/06
Nález Ústavního soudu ČR ze dne 15. března 2005, sp. zn. I. ÚS 367/03
Nález Ústavního soudu ČR ze dne 23. března 2010, sp. zn. I. ÚS 1990/08
Nález Ústavního soudu ČR ze dne 9. prosince 2014, sp. zn. II. ÚS 1774/14
Nález Ústavního soudu ČR ze dne 12. října 1994, sp. zn. Pl. ÚS 4/94
Nález Ústavního soudu ČR ze dne 18. dubna 1995, vyhlášený pod č. 55/1995 Sb.
Nález Ústavního soudu ČR ze dne 27. února 1997, vyhlášený pod č. 24/1997 Sb.
Rozhodnutí Ústavního soudu ČR ze dne 7. listopadu 2012, sp. zn. I. ÚS 3933/12
Rozhodnutí Nejvyššího správního soudu ČR ze dne 20. prosince 2018, sp. zn. 6 As 168/2018
Rozhodnutí Nejvyššího správního soudu ČR ze dne 25. února 2015, sp. zn. 1 As 113/2012
Rozhodnutí Nejvyššího správního soudu ČR ze dne 23. srpna 2013, sp. zn. 5 As 158/2012
Rozhodnutí Nejvyššího správního soudu ČR ze dne 14. srpna 2015, sp. zn. 5 As 10/2015
Rozhodnutí Nejvyššího správního soudu ČR ze dne 19. září 2014, sp. zn. 4 As 123/2014
Rozhodnutí Nejvyššího správního soudu ČR ze dne 17. července 2018, sp. zn. 3 As 3/2017
Rozhodnutí Nejvyššího správního soudu ČR ze dne 12. února 2009, sp. zn. 9 As 34/2008
Rozhodnutí Nejvyššího správního soudu ČR ze dne 28. června 2013, sp. zn. 5 As 1/2011
rozhodnutí Městského soudu v Praze ze dne 16. 10. 2012, sp. zn. 6 Ca 378/2008
Rozhodnutí Městského soudu v Brně ze dne 28. února 2007, sp. zn. 7 Ca 204/2005
Rozhodnutí ÚOOÚ ze dne 29.5.2008, č. j. SKO-0629/07

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

Rozhodnutí SDEU ze dne 6. listopadu 2003, C-101/01, ve věci Bodil Lindqvist

Rozhodnutí SDEU ze dne 20. října 2016, C-582/14, ve věci Patrick Breyer v. Bundesrepublik Deutschland

Rozhodnutí SDEU, ze dne 20. května 2003, ve spojených věcech C-465/00, C-38/01 a C-139/01

Rozhodnutí SDEU ze dne 13. května 2014, C-131/12, ve věci Google Spain

Rozhodnutí ESLP ze dne 25. června 1997 ve věci Halford vs. Spojené království, č. stížnosti 20605/92

Rozhodnutí ESLP ze dne 4. května 2000, ve věci Rotaru v. Rumunsko, č. stížnosti 28341/95

Rozhodnutí ESLP ze dne 16. února 2000 ve věci Amann vs. Švýcarsko, č. stížnosti 27798/95

Rozhodnutí ESLP ze dne 3. července 2007 ve věci Copland vs. Spojené království, č. stížnosti 62617/00

Rozhodnutí ESLP ze dne 16. září 2008, ve věci Pay v. Spojené království, č. stížnosti 32792/05

Rozhodnutí ESLP ze dne ze dne 5. března 2018 ve věci Akhlyustin vs. Rusko, č. stížnosti 21200/05

Rozhodnutí ESLP ze dne 7. července 1989, ve věci Gaskin v. Spojené království, č. stížnosti 10454/83

Rozhodnutí ESLP ze dne 25. února 1997 ve věci Z. vs. Finsko, č. stížnosti 22009/93

Rozhodnutí ESLP ze dne 5. října 2010 ve věci Köpke vs. Německo, č. stížnosti 420/07

Rozhodnutí ESLP ze dne 13. ledna 2015 ve věci Rubins vs. Lotyšsko, č. stížnosti 79040/12

Rozhodnutí ESLP ze dne 17. října 2003 ve věci Perry vs. Spojené království, č. stížnosti 63737/00

Rozhodnutí ESLP ze dne 26. října 2007 ve věci Peev vs. Bulharsko, č. stížnosti 64209/01

Rozhodnutí ESLP ze dne 24. dubna 2018 ve věci Benedik vs. Slovinsko, č. stížnosti 62357/14

Rozhodnutí ESLP ze dne 12. ledna 2016 ve věci Barbulescu vs. Rumunsko, č. stížnosti 61496/08

Rozhodnutí Velkého senátu ESLP ze dne 5. září 2017 ve věci Barbulescu vs. Rumunsko, č. stížnosti 61496/08

Rozhodnutí ESLP ze dne 28. listopadu 2017 ve věci Antonović a Mirković vs. Černá hora, č. stížnosti 70838/13

Rozhodnutí německého federálního pracovního soudu (*Bundesarbeitsgericht*) ze dne 27. července 2017, sp. zn. 2 AZR 681/16

Rozhodnutí německého krajského pracovního soudu (*Landesarbeitsgericht)* ze dne 14. ledna 2016, sp. zn. 5 Sa 657/15

Seznam ostatních zdrojů

Stanovisko ÚOOÚ č. 2/2001: *Zpracování citlivého osobního údaje o členství v odborových organizacích v souvislosti s odváděním členských příspěvků členů odborových organizací*. Říjen 2001, aktualizováno červenec 2006, červen 2007, revize srpen 2009.

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

Stanovisko ÚOOÚ č. 2/2009: *Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště*. Únor 2009.

Stanovisko ÚOOÚ č. 6/2009: *Ochrana soukromí při zpracování osobních údajů*. Listopad 2009, aktualizace únor 2014.

Stanovisko ÚOOÚ č. 2/2011: *Zpracování osobních údajů na základě souhlasu ve smlouvě nebo Všeobecných obchodních podmínkách a s tím související problémy*. Srpen 2011, aktualizace únor 2014.

Stanovisko ÚOOÚ č. 6/2012: *Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů*. Březen 2012, poslední revize duben 2013.

Stanovisko ÚOOÚ č. 3/2014: *K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti*. Srpen 2014.

Stanovisko ÚOOÚ č. 1/2017: *Biometrická identifikace nebo autentizace zaměstnanců*. Červen 2017.

Stanovisko WP29 č. 4/2004: Ke zpracování osobních údajů prostřednictvím kamerového sledování (v originále: *opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance)*. (WP89), ze dne 11. února 2004.

Stanovisko WP29 č. 8/2001: Zpracování osobních údajů v kontextu zaměstnání (v originále: *opinion 8/2001 on the processing of personal data in the employment context*). (WP48), ze dne 13. září 2001.

Pracovní dokument WP29: Ke sledování elektronických komunikací na pracovišti (v originále: *Working document on the surveillance of electronic communications in the workplace*). (WP55), ze dne 29. května 2002.

Stanovisko WP29 č. 1/2006: K aplikaci pravidel ochrany osobních údajů na whistleblowing (v originále: *opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime)*. (WP117), ze dne 1. února 2006.

Stanovisko WP29 č. 1/2010: Ke konceptům „správce“ a „zpracovatel“ (v originále: *opinion 1/2010 on the concepts of "controller" and "processor")*. (WP169), ze dne 16. února 2010.

Stanovisko WP29 č. 13/2011: Ke geolokalizačním službám u inteligentních mobilních zařízení (v originále: *opinion 13/2011 on Geolocation services on smart mobile devices)*. (WP185), ze dne 16. května 2011.

Stanovisko WP29 č. 15/2011: K definici souhlasu (v originále: *opinion 15/2011 on the definition of consent*). (WP187), ze dne 13. července 2011.

Stanovisko WP29 č. 3/2013: K účelovému omezení (v originále: *opinion 3/2013 on purpose limitation).* (WP203), ze dne 2. dubna 2013.

Stanovisko WP29 č. 5/2014: K technikám anonymizace (v originále: *opinion 5/2014 on Anonymisation Techniques).* (WP216), ze dne 10. dubna 2014.

Stanovisko WP29 č. 6/2014: K pojmu oprávněných zájmů správce podle článku 7 směrnice 95/46/ES (v originále: *opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC).* (WP217), ze dne 9. dubna 2014.

Stanovisko WP29 č. 2/2017: Zpracování údajů na pracovišti (v originále: *opinion 2/2017 on data processing at work).* (WP249), ze dne 8. června 2017.

WP29: *Pokyny týkající se práva na přenositelnost údajů*. (WP242 rev. 01), vydané dne 13. prosince 2016, ve znění ze dne 5. dubna 2017.

WP29: *Pokyny týkající se pověřenců pro ochranu osobních údajů*. (WP 243 rev. 01), vydané dne 13. prosince 2016, ve znění ze dne 5. dubna 2017.

WP29: *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679*. (WP 248 rev. 01), vydané dne 4. dubna 2017, ve znění ze dne 4. října 2017.

WP29: *Pokyny pro souhlas podle nařízení 2016/679*. (WP 259 rev. 01), vydané dne 28. listopadu 2017, v revidovaném znění ze dne 10. dubna 2018.

WP29: *Pokyny k transparentnosti podle nařízení 2016/679*. (WP 260 rev. 01), vydané dne 29. listopadu 2017, ve znění ze dne 11. dubna 2018.

Poslanecká sněmovna ČR, Vláda ČR: Důvodová zpráva k zákonu č. 89/2012 Sb., občanský zákoník, a další související zákony (konsolidované znění).

Poslanecká sněmovna ČR, Vláda ČR: Důvodová zpráva k zákonu č. 110/2019 Sb., zákon o zpracování osobních údajů.

Přednášky účastníků na konferenci Nové příležitosti a meze uplatnění alternativních řešení sporů v České republice, konané dne 4. a 5. listopadu 2016, na Právnické fakultě Univerzity Karlovy.

Konzultace s vybranými právními poradci z různých evropských zemí v rámci konference WSG (World Services Group) v Rize, Lotyšsko, konané dne 8. a 9. března 2018.

Konzultace s vybranými právními poradci z různých evropských zemí v rámci konference WSG (World Services Group) v Lisabonu, Portugalsko, konané dne 21. a 22. března 2019.

Abstrakt

Ochrana osobnosti a osobních údajů v pracovněprávních vztazích

Disertační práce se zabývá tématem ochrany osobnosti a osobních údajů v pracovněprávních vztazích. Jedná se o velice aktuální téma, neboť rozvoj informačních technologií umožňuje snazší zasahování do soukromí zaměstnanců ze strany jejich zaměstnavatelů. Široké využití informačních technologií a související automatizace procesů na pracovišti umožňují v dnešní době snadné monitorování výkonu zaměstnance, sledování toho, kdy čerpá pauzy a jak je tráví, jak spolupracuje s ostatními zaměstnanci nebo jak využívá svěřené prostředky. Kromě toho k popularitě tématu v poslední době přispěla rovněž nová regulace ochrany osobních údajů, a to v podobě obecného nařízení o ochraně osobních údajů (GDPR). Toto nařízení sice nepřináší mnoho právních novinek oproti předchozí právní úpravě, ale zásadně zpřísňuje postih za porušení stanovených pravidel.

Práce je systematicky rozčleněna celkem do 4 částí, přičemž první z částí se zabývá právním rámcem a právními prameny analyzované problematiky a dále popisuje obecná východiska pro zkoumání ochrany osobnosti, včetně ochrany soukromí a ochrany osobních údajů, což je nezbytné pro výklad podaný v dalších částech. Druhá část se věnuje již samostatně ochraně osobnosti a soukromí zaměstnanců. Pozornost je věnována specifikům vztahů mezi zaměstnanci a zaměstnavateli, relevantní judikatuře, ochraně zaměstnanců před a po skončení pracovního poměru či možnostem kontrol a sledování zaměstnanců, a to na pracovišti i mimo něj. Třetí část se dále věnuje specifickým otázkám vyplývajícím z regulace ochrany osobních údajů. Zejména jsou zkoumány právní základy pro zpracování osobních údajů zaměstnanců, související práva zaměstnanců, možnosti zpracování jednotlivých údajů a dodržování dalších zásad stanovených nařízením GDPR ze strany zaměstnavatelů. Čtvrtá část obsahuje analýzu vybraných aplikačních otázek, kterými jsou především jednotlivé nástroje monitoringu nejčastěji využívané v praxi zaměstnavateli, jako jsou kamery, sledování GPS, sledování využívání internetu apod. Nabídnut je rovněž pohled na vybrané zahraniční právní úpravy a na závěr jsou poskytnuty úvahy *de lege ferenda*.

Klíčová slova: GDPR, ochrana osobnosti, osobní údaje, zaměstnanci

Abstract

Personality and personal data protection in employment law relationships

This dissertation deals with the topic of personality and personal data protection in employment law relationships. This is a very topical subject, as the development of information technology has made it easier for employers to infringe on their employees' privacy. Today, the widespread use of information technology and the related process automation in the workplace makes it easy to monitor employee performance, to track when an employee takes a break and how long it lasts, to monitor how the employee cooperates with other employees, and how the employee uses entrusted resources. Apart from that, a new regulation on personal data protection has also recently contributed to the popularity of the topic: the adoption of the General Data Protection Regulation (GDPR). Although this regulation does not bring many new legal rules compared to the previous legislation, it severely and significantly toughens the penalties for violating the rules.

This dissertation is divided into 4 parts. The first part deals with the legal framework and legal sources of the analysed topic and further describes the general basis for examining the personality protection, including privacy protection, and the protection of personal data, which is essential for the interpretation given in other parts. The second part deals with the personality and privacy protection of employees. Attention is paid to the specifics of the relationship between employees and employers, relevant case law, protection of employees before and after their employment relationship, and the possibility of controlling and monitoring employees, both inside and outside the workplace. The third part deals with specific issues arising from the regulation of personal data protection. In particular, the legal basis for processing employees' personal data, related employees' rights, possibilities of individual data processing and employers' adherence to other principles set by the GDPR are examined. The fourth part contains an analysis of selected practical issues, which are mainly the monitoring tools most frequently used by employers in practice, such as cameras, GPS tracking, internet usage monitoring etc. Selected foreign legislations are also analysed and *de lege ferenda* considerations are provided at the end.

Key words: GDPR, personality protection, personal data, employees