UNIVERZITA KARLOVA

Právnická fakulta

Andrea Drozdíková

Monitoring zaměstnanců

Diplomová práce

Vedoucí diplomové práce: doc. JUDr. Martin Štefko, Ph.D.

Katedra: Pracovního práva a práva sociálního zabezpečení

Datum vypracování práce (uzavření rukopisu): 2. 5. 2018

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala 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 131 566 znaků včetně mezer.

diplomantka

V Praze dne

Poděkování

Ráda bych tímto poděkovala vedoucímu této diplomové práce, panu doc. JUDr. Martinovi Štefkovi, Ph.D., a to jak za samotné vedení diplomové práce, tak i za cenné připomínky, rady a pomoc při zpracování.

Obsah

1. Úvod ... 1

2. Právo na soukromí ... 3

2.1. Prameny mezinárodního práva ... 3

2.2. Ochrana soukromí – česká právní úprava ... 4

2.2.1. Listina základních práv a svobod ... 5

2.2.2. Občanský zákoník ... 5

2.2.3. Zákon o ochraně osobních údajů ... 6

2.2.4. Trestní zákoník ... 8

2.3. Ochrana soukromí zaměstnance ... 10

2.3.1. Pojem soukromí ... 10

2.3.2. Zákoník práce ... 12

2.3.3. Zákon o inspekci práce ... 13

3. Právo vlastnit majetek, ochrana majetku ... 14

3.1. Prameny mezinárodního práva ... 14

3.2. Vnitrostátní právní úprava ... 14

3.2.1. Listina ... 14

3.2.2. Občanské právo ... 15

3.3. Ochrana majetku zaměstnavatele ... 15

3.3.1. Povinnost používat majetek k pracovním účelům ... 15

3.3.2. Povinnost zaměstnance odvrátit škodu ... 18

3.4. Právo na ochranu majetku zaměstnavatele ... 18

4. Monitoring zaměstnanců ... 20

4.1. Legitimní důvody – stanovení účelu monitoringu ... 22

4.1.1. Zpracování se souhlasem zaměstnance ... 23

4.1.2. Zpracování bez souhlasu zaměstnanců ... 24

4.2. Povinnosti zaměstnavatele spojené s monitoringem ... 26

4.2.1. Zásada proporcionality ... 26

4.2.2. Informační povinnost ... 28
4.2.3. Oznamovací (registrační) povinnost ... 29
4.2.4. Povinnost zabezpečit osobní údaje ... 30
4.3. Jednotlivé formy monitoringu ... 31
4.3.1. Kontrola e-mailové a obdobné elektronické korespondence ... 31
4.3.2. Monitoring telefonů ... 36
4.3.3. Monitoring aktivity na PC ... 37
4.3.4. Kamery na pracovišti ... 40
4.3.5. Kamera v kabině auta ... 41
4.3.6. Kontrola docházky na pracoviště ... 43
4.3.7. Monitoring pomocí GPS ... 47
4.4. Další formy kontroly – monitoring zaměstnance klientem zaměstnavatele ... 50
5. Porovnání s úpravou Velké Británie ... 51
5.1. Úvod ... 51
5.2. Soukromí „anglického“ zaměstnance ... 52
5.2.1. Ochrana osobních údajů ... 54
5.2.2. Monitoring zaměstnanců ... 56
5.3. Závěr k porovnání s úpravou Velké Británie ... 58
6. Závěr ... 59
Seznam nejčastěji použitých zkratek ... 63
Seznam použité literatury a zdrojů ... 64
Abstrakt ... 71
Abstract ... 73

1. Úvod

Téma ochrany soukromí (nejen) v zaměstnání rezonuje jak v odborné literatuře, tak v oblasti legislativní. Odborníci (napříč právními řády) se shodují, že soukromí se v moderní době v důsledku nevídaného technologického pokroku stalo jedním z nejdůležitějších lidských práv a jeho ochrana klíčová.[1] Zvolené téma diplomové práce se, jak vyplývá ze samotného názvu, zaobírá problematikou sledování, monitorování zaměstnanců (nejen) na pracovišti. Tato problematika tedy jistě představuje aktuální téma, kterému se věnuje čím dál tím více pozornosti.

Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „*ZP*"), proto zaměstnance před neoprávněným a nepřiměřeným zásahem do soukromí výslovně chrání. Zároveň ale také přiznává zaměstnavateli v určitých situacích možnost monitoring svých zaměstnanců provádět.

Na aktuálnost problematiky ochrany soukromí v oblasti legislativy, a to zejména prostřednictvím ochrany zpracování osobních údajů, dále poukazuje např. i přijetí nového obecného evropského nařízení o ochraně osobních údajů (dále jen „*GDPR*"),[2] které nabude účinnosti dne 25. května 2018. Ačkoliv Asociace kolektivního vyjednávání nespatřuje v přijetí tohoto nařízení pro zaměstnavatele nic obzvláště přelomového,[3]

[1] Např. Davies v DAVIES, S. *New Techniques and Technologies of Surveillance in the Workplace* via COLLINS, H., EWING, K.D., a McCOLGAN, A. *Labour Law: Text and Materials.* 2. vydání. Portland, Oregon. Hart Publishing, 2005, s. 601: "*Privacy has become one of the most important human right issue of the modern age. Privacy has become a crucial safeguard for individual rights."* Z českého prostředí pak Nejvyšší správní soud ve svém rozsudku sp. zn. 9 As 34/2008 ze dne 12. 2. 2009. Dále pak obdobně např. Morávek v MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, str. 15 a také BÁRTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi (vybrané problémy).* 4. vydání. Praha: Wolters Kluwer ČR, 2016, s. 128

[2] 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)

[3] Zápis z jednání Kolegia expertů AKV konaného v Kolíně ve dnech 3. a 4. 11. 2017

faktem je, že ochrana osobních údajů by nyní měla být propracovanější, a především sankce za porušení by měly být závažnější.[4]

Práce se skládá celkově ze šesti kapitol, včetně úvodu a závěru. Po této první úvodní kapitole se druhá věnuje právnímu rámci ochrany soukromí, resp. ochrany osobních údajů subjektů, a to nejprve obecně a posléze speciálně ve vztahu ke speciálním subjektům – tj. ochraně dat zaměstnanců a jejich soukromí na pracovišti. S ohledem na zaměření této práce a její limitovaný rozsah pak bude v otázce zpracování osobních údajů upřena pozornost jen na zpracování osobních údajů při trvání pracovněprávního vztahu, a to pouze z důvodu monitoringu.[5] Ze stejného důvodu je ponechán stranou pozornosti též zákaz vyžadování informací, které přímo nesouvisejí s výkonem práce, který je jinak obsahem stejného ustanovení ZP, které se věnuje monitoringu zaměstnanců, a dále také práce nerozebírá úpravu předávání osobních údajů do zahraničí.

Třetí kapitola při stejném postupu obdobně přibližuje nejprve právní úpravu ochrany vlastnictví a majetku obecně a následně speciální úpravu ochrany majetku patřícího zaměstnavateli.

Čtvrtou část lze považovat za jakési gros práce, neboť se nejprve zaměřuje na legitimní důvody opravňující zaměstnavatele provádět monitoring zaměstnanců, tedy zda může zaměstnavatel zpracovávat osobní údaje zaměstnanců s jejich souhlasem, či bez něj, dále přibližuje s monitoringem spojené povinnosti zaměstnavatele a konečně se pak kapitola věnuje vybraným konkrétním formám kontroly pracovníků, tedy právně přípustnému zásahu do soukromí zaměstnance. Nejprve je věnována pozornost sledování na pracovišti, resp. v prostorách zaměstnavatele[6], pak i mimo tyto prostory. Ve čtvrté kapitole jsou tak popsány a podrobněji rozebrány jednotlivé formy kontrol a diskutovány hranice legálních možností monitoringu zaměstnanců. V této kapitole je zejména

[4] Blíže k sankcím níže v příslušné kapitole č. 3.

[5] Tedy nikoliv již na zpracování osobních údajů před vznikem a po skončení pracovních poměrů, jak tuto oblast rozdělil JUDr. Morávek ve své knize MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, část IV.

[6] Pracovištěm zaměstnance se pro účely této práce myslí prostory zaměstnavatele, ve kterých zaměstnanec vykonává práci. Jedná se tedy o jakýsi střední rozsah významu pracoviště ve vztahu k vymezení pracoviště ve stanovisku Úřadu pro ochranu osobních údajů č. 2/2009, kdy podle tohoto je širším významem myšleno místo výkonu práce, příp. celá obec a užším významem je pak pracovní stůl zaměstnance a bezprostřední pracovní okolí.

zmiňována a přiblížena judikatura vztahující se k dané problematice. Přestože není příliš rozsáhlá, několik bezesporu zajímavých rozhodnutí již existuje.

Pátá kapitola pak přináší exkurz do zahraniční právní úpravy, konkrétně do právního řádu Velké Británie, a to jak deskripci toho, jak je zde tato problematika pojímána, tak i nabízejícího se srovnání s českou právní úpravou. Autorka práce se totiž danou problematikou zabývala i při studijním pobytu ve Velké Británii v rámci programu Erasmus+.

Cílem práce je přiblížit právní úpravu věnovanou dané problematice a pokusit se i na již rozhodnutých soudních sporech pomyslně načrtnout, kde leží hranice legálnosti monitoringu a kdy už se zaměstnavatel pohybuje mimo mez zákona. Daná problematika se totiž týká posouzení střetu dvou významných práv – práva na ochranu majetku (zaměstnavatele) a práva na ochranu soukromí (zaměstnance).

Pro zpracování diplomové práce budou použity především metody popisu, analýzy a také srovnání.

2. Právo na soukromí

2.1. Prameny mezinárodního práva

Jak již bylo zmíněno v úvodu, prvním ze dvou základních práv, kolidujících si navzájem při provádění monitoringu zaměstnanců, je právo na ochranu soukromí člověka. Základní rámec lze nalézt na mezinárodní úrovni ve vícero úmluvách. První z nich je např. Mezinárodní pakt o občanských a politických právech (dále jen „*MPOPP*“)[7], který v čl. 17 odst. 1 stanoví zákaz svévolného zasahování do soukromého či rodinného života, domova nebo korespondence a taktéž zakazuje útoky na čest a pověst.

[7] Vyhláška ministra zahraničních věcí č. 120/1976 Sb., o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech.

Následuje evropská Úmluva o ochraně lidských práv a základních svobod (dále jako „*EÚLP*“)[8], která zakotvuje obdobné pravidlo ve svém čl. 8, v němž je stanoveno právo na respektování soukromého a rodinného života a taktéž obydlí a korespondence. Zatímco druhý odstavec čl. 17 MPOPP hovoří o právu domáhat se zákonné ochrany proti zakázaným zásahům, druhý odstavec čl. 8 EÚLP rozvádí případy, kdy státní orgán může do chráněného soukromí zákonně zasáhnout. Jedná se zejména o situace, kdy je to nezbytné v demokratické společnosti, v zájmu národní a veřejné bezpečnosti, dále pro ochranu zdraví či ochranu práv a svobod jiných aj.[9]

Dalším pramenem je pak čl. 1 Směrnice Evropského parlamentu a Rady č. 95/46/ES (dále jen „*Směrnice*“)[10], který ukládá členským státům Evropské unie zajistit na vnitrostátní úrovni ochranu soukromí fyzických osob. Tato Směrnice však bude s účinností od 25. května 2018 nahrazena již v úvodu zmíněným nařízením GDPR. I po tomto datu však zůstane účinná Listina základních práv Evropské unie[11], která v čl. 7 stanoví právo každého na respektování jeho soukromého a rodinného života. Tedy i po zrušení Směrnice zůstává na půdě Evropské unie právně zakotvené právo na ochranu soukromí.

2.2. Ochrana soukromí – česká právní úprava

Jak patrno z předchozí části kapitoly, mezinárodní úprava poměrně hojně pamatuje na právo na ochranu soukromí. Vnitrostátní právní úprava v tomto ohledu ovšem nijak nezaostává.

[8] Sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících, ve znění pozdějších předpisů.

[9] To však neznamená, že by právo na ochranu práv bylo v EÚLP opomenuto. Tomuto se věnuje čl. 6 EÚLP a dále čl. 34 EÚLP, který přiznává pravomoc Evropskému soudu pro lidská práva (sídlícímu ve Štrasburku), rozhodovat o stížnosti každého, který má za to, že byl poškozen v důsledku porušení práv přiznaných mu touto úmluvou. Díky tomuto ustanovení tak právo na ochranu soukromí není v EÚLP pouze jednostranně proklamováno, ale je zajištěna jeho ochrana prostřednictvím rozhodování soudního orgánu.

[10] 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.

[11] Listina základních práv Evropské unie ze dne 7. 12. 2000, ve znění upraveném dne 12. 12. 2007 ve Štrasburku, právně závazná prostřednictvím přijetí tzv. Lisabonské smlouvy účinné od 1. 12. 2009.

2.2.1. Listina základních práv a svobod

Na ústavní úrovni je respekt k soukromí člověka zakotven v Listině základních práv a svobod (dále jen „*Listina*“)[12] v jejím čl. 7., který zaručuje nedotknutelnost osoby a jejího soukromí, tyto lze omezit jen zákonem. Toto právo je dále v Listině rozvedeno, kdy čl. 10 odst. 2) Listiny stanoví právo každého na ochranu před neoprávněným zásahem do soukromí a rodinného života a čl. 10 odst. 3) Listiny pak vyslovuje ochranu před neoprávněným shromažďováním osobních údajů. Čl. 13 Listiny pak zaručuje ochranu písemností a záznamů, tedy ochranu listovního tajemství a obdobné soukromé korespondence. Chráněn je nejen obsah této korespondence, ale i další informace vztahující se ke korespondenci – jako např. údaj o volaném čísle, datum a čas hovoru, doba trvání hovoru atd.).[13] Odborná literatura uvádí, že výjimky z této ochrany jsou povoleny pouze z důvodu veřejného zájmu, jakým je například ochrana před páchání trestné činnosti,[14] nicméně dále se lze dočíst, a to s odkazem na judikaturu českých a evropských soudů, že ve vztahu k počtu odeslaných a přijatých e-mailových zpráv a údajům o adresách odesílatelů lze monitoring provádět bez dalšího.[15] K tomu však blíže v příslušné podkapitole 4.3.1.

2.2.2. Občanský zákoník

Pracovní právo sice je samostatným odvětvím práva soukromého,[16] nicméně s ohledem na znění § 4 ZP je potřeba pamatovat i na úpravu v občanském právu,

[12] Listina základních práv a svobod, vyhlášená zákonem č. 23/1991 Sb., kterým se uvozuje LISTINA ZÁKLADNÍCH PRÁV A SVOBOD jako ústavní zákon Federálního shromáždění České a Slovenské Federativní Republiky, republikovaná usnesením předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění ústavního zákona č. 162/1998 Sb., kterým se mění Listina základních práv a svobod

[13] Viz nález Ústavní soudu ČR sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001.

[14] BĚLINA, M. a kol.: *Pracovní právo. 7. doplněné a podstatně přepracované vydání*. Praha: C. H. Beck, 2017, s. 166

[15] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1244

[16] BĚLINA, M. a kol.: *Pracovní právo. 7. doplněné a podstatně přepracované vydání*. Praha: C. H. Beck, 2017, s. 4

neboť na pracovněprávní vztahy se subsidiárně může použít i zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „*ObčZ*“),[17] samozřejmě s pamatováním na základní zásady pracovního práva. Je tedy na místě podívat se na úpravu dané oblasti i v rámci ObčZ. Krom toho, že je v úvodních ustanoveních v § 3 odst. 2 písm. a) ObčZ stanovena základní zásada soukromého práva chránit soukromí každého, jsou dále ochraně soukromí věnovány § 81 an. ObčZ, kdy tyto hovoří o zákonné ochraně osobnosti člověka, včetně jeho přirozených práv, jedním z nich je právo na soukromí. Podle § 86 ObčZ nikdo nemůže zasáhnout do soukromí jiného, aniž by k tomu měl zákonný důvod, zejména pak nelze bez souhlasu dotyčného narušit jeho soukromí, sledovat jeho soukromý život a pořizovat o tomto zvukový nebo obrazový záznam. Ve stejném rozsahu jsou chráněny písemnosti osoby. Ustanovení § 88 ObčZ pak dovoluje pořizovat tyto záznamy zasahující do soukromí, jestliže je tak činěno z důvodu výkonu nebo ochrany jiných práv, či právem chráněných zájmů jiných osob. Ustanovení § 90 ObčZ pak přibližuje povinnost přiměřeného postupu, je-li do soukromí osoby zasaženo ze zákonného titulu.

2.2.3. Zákon o ochraně osobních údajů

V oblasti soukromého práva je dále upravena ochrana soukromí osoby ještě v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „*ZOOÚ*“), kdy hned § 1 ZOOÚ vymezuje účel dané zákonné úpravy, kterým je naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí a regulace práv a povinností při zpracování osobních údajů. ZOOÚ se na příslušnou situaci aplikuje, dochází-li ke zpracování osobních údajů ve smyslu podle ZOOÚ.[18] Vedle situace, kdy při sledování zaměstnanců dochází ke zpracování jejich osobních údajů, která je regulována jak ZP, tak ZOOÚ, literatura popisuje také situace, kdy k aplikaci ZP vůbec nedojde a tato bude regulována pouze skrze ZOOÚ. Jednat by se mělo např.

[17] Stojí za zmínku, že princip subsidiarity ve vztahu k ObčZ nahradil s účinností od 1. 1. 2012 předcházející princip delegace, a to novelou zákona č. 365/2011 Sb.

[18] NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 232

o jednorázový vstup do e-mailové schránky zaměstnance, či monitorování vstupu do určitých prostor přístupovým systémem.[19]

Podle § 4 písm. j) ZOOÚ se správcem rozumí „*každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj*." Zaměstnavatel se tedy při vzniku pracovněprávního vztahu stává správcem osobních údajů.[20] Jako správci mu pak ZOOÚ ukládá řadu povinností, obecnou povinnost k respektování soukromí a ochranu před neoprávněným zásahem do tohoto nalezneme v § 11 ZOOÚ.

Zaměstnancovo soukromí je tedy chráněno, a to např. efektivně prostřednictvím správních postihů ukládaných zaměstnavateli. Zaměstnanec se může při podezření na neoprávněný zásah do svého soukromí obrátit s podnětem na Úřad pro ochranu osobních údajů (dále jen „*ÚOOÚ*") a tento pak může při zjištění porušení povinností s odkazem na § 45 ZOOÚ uložit pokutu ve výši až 5.000.000 Kč. Sezná-li ÚOOÚ, že při zpracování osobních údajů došlo k ohrožení většího počtu osob neoprávněným zásahem do jejich soukromého a osobního života, což jistě při nelegálním monitoringu hrozí, pak se výše pokuty navyšuje až na částku 10.000.000 Kč.[21] Po nabytí účinnosti GDPR[22] bude možné za porušení povinností spojených s ochranou osobních údajů uložit nově pokutu až do výše 2.000.000 EUR, či až do výše 4 % obratu podniku,[23] a to podle toho, která z těchto bude vyšší.[24] Z nedávno předloženého vládního návrhu zákona o zpracování osobních údajů[25] však plyne, stihne-li tento nabýt účinnosti ještě před zmiňovaným 25. květnem 2018,

[19] Tamtéž, s. 233

[20] Viz stanovisko ÚOOÚ č. 6/2012 – Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů, aktuální verze ze dne 21. 3. 2013, s. 1

[21] Tato zvýšená částka pokuty platí podle § 45 ZOOÚ i pro porušení povinností při zpracovávání citlivých osobních údajů. Evidence docházky se záměrem využívat biometrické údaje zaměstnanců přitom není nic neslýchaného. Blíže k tomu viz podkapitola 4.3.6.

[22] Od data 25. května 2018.

[23] Podnik chápán ve smyslu článků 101 a 102 Smlouvy o fungování EU Úřední věstník C 326, ze dne 26. 10. 2012, s. 1 – 390

[24] Čl. 83 GDPR

[25] Čj. OVA 55/18, sněmovní tisk č. 138/0, 8. volební období, od roku 2017, ve znění z 9. 4. 2018

že maximální výše pokuty pro některé vybrané přestupky při zpracování osobních údajů bude i nadále maximálně 10.000.000 Kč.[26]

Potud uvedená právní úprava je tedy ve vztahu k ochraně soukromí zaměstnanců subsidiárně použitelná, neboť zaměstnanec na pracovišti je pořád zejména osoba a člověk, jehož soukromí právo respektuje a chrání.[27] Dále lze zhodnotit, že se v jednotlivých oblastech – občanské právo, právní úprava zpracování osobních údajů atd., základní zásady a pravidla nijak neliší, často je i samotná textace velice podobná.

2.2.4. Trestní zákoník

Nabízí se otázka, zda je soukromí zaměstnance (jakožto soukromí osoby) před neoprávněným zásahem zaměstnavatele chráněno také obecnou úpravou v zákoně č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále jen „*TZ*“). Při pohledu na obsah jednotlivých relevantních skutkových podstat v Dílu 2 Hlavy II. Zvláštní části TZ[28] lze vyslovit názor, že spíše nikoliv.[29] Literatura upozorňuje, že dané skutkové podstaty svým zaměřením cílí na jiné situace, než je neoprávněný zásah zaměstnavatele do soukromí zaměstnance, jakým může být např. nedovolené pročítání e-mailové korespondence, či odposlech soukromého rozhovoru mezi zaměstnanci. V této souvislosti je dále zmíněn rozsudek Nejvyššího soudu sp. zn. 11 Tdo 349/2009,[30] ve kterém Nejvyšší soud upřesnil, že ochrana e-mailové korespondence je poskytována ve vztahu k procesu doručování, upravena tímto tedy není doba po okamžiku doručení e-mailu. Daní autoři v tomto směru konstatují nedostatky právní úpravy, neboť trestní právo by jako velice efektivní nástroj ochrany práv podle jejich názoru mělo obsahovat možnost postihnout

[26] Tamtéž, s. 28 – 30, příslušné § 60 – 62.

[27] BĚLINA, M. a kol.: *Pracovní právo. 7. doplněné a podstatně přepracované vydání*. Praha: C. H. Beck, 2017, s. 166

[28] Trestným činem je totiž podle § 13 TZ pouze takový protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně.

[29] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců.* 1. vydání. Praha: C.H. Beck, 2013, s. 39 an.

[30] Rozsudek Nejvyššího soudu sp. zn. 11 Tdo 349/2009, ze dne 21. 5. 2009, publikováno pod T 1197 v Souboru trestních rozhodnutí a stanovisek Nejvyššího soudu ČR.

neoprávněný monitoring zaměstnanců obecně, nikoliv jen v určitých, z pohledu monitoringu zaměstnanců minoritních, specifických situacích.[31] V tomto ohledu je zmíněn v minulosti navrhovaný § 180a TZ[32].

Zmíněné ustanovení mělo upravovat skutkovou podstatu trestného činu tzv. „Nedovoleného sledování“.[33] Relevantní sněmovní tisk neprošel celým legislativním procesem, v Poslanecké sněmovně bylo projednávání přerušeno a následně ukončeno s koncem volebního období.[34] K návrhu této novely zákona se tak Poslanecká sněmovna a logicky tedy ani Senát skrze svá usnesení nijak nevyjádřily. Vláda ve svém stanovisku s navrženou novelizací nesouhlasila.[35] Mimo jiné vyjádřila názor, že případy takového nedovoleného sledování jsou již chráněny právem občanským a částečně právě i právem trestním. Dále vláda rozporovala zejména použitou terminologii. Lze tedy uzavřít, že tehdejší vláda nevnímala mezery v trestním právu tak, jak o nich píši autoři citované publikace.[36]

Konečně pak ve vztahu k pracovnímu právu lze nalézt speciální úpravu ochrany soukromí přímo v pracovněprávních předpisech, jimž je věnována samostatná podkapitola níže.

---

[31] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců.* 1. vydání. Praha: C. H. Beck, 2013, s. 39 an., zejm. s. 41.

[32] Navrhované znění předmětného §180a lze nalézt ve sněmovním tisku č. 428 ze 6. období Poslanecké sněmovny (2010 – 2013).

[33] Neoprávněného sledování se měl podle navrženého §180a odst. 1) TZ dopustit ten „*kdo neoprávněně a v rozporu s veřejným zájmem o jiném, nebo o jeho věcech utajovaným způsobem získává poznatky s použitím elektronického nebo jiného technického zařízení“* a dále ten, kdo takový čin *„sjedná, nebo o něj požádá, nebo jej zajistí*.“

[34] Viz veřejně dostupné informace na stránkách Poslanecké sněmovny Parlamentu České republiky ke sněm. tisku č. 428, ze 6. období Poslanecké sněmovny (2010 – 2013)

[35] Viz předmětné stanovisko vlády, sněmovní tisk č. 428/1, ze 6. období Poslanecké sněmovny (2010 – 2013)

[36] Autorka diplomové práce se tímto nepřiklání k jednomu, či druhému názoru, pouze upozorňuje na různé pohledy na danou problematiku.

2.3. Ochrana soukromí zaměstnance

2.3.1. Pojem soukromí

Ještě než přejdeme k samotné právní úpravě, pozastavíme se nad otázkou, kterou odborná literatura vznáší, a sice co to je soukromí a existuje vůbec na pracovišti?[37] Na první pohled možná nadbytečná otázka, ale ve svém důsledku může tato, řekněme proměnná veličina soukromí na pracovišti, rozhodnout o oprávněnosti postupu zaměstnavatele.[38] Rozsah stanovené ochrany soukromí se totiž liší s ohledem na charakter prostor, ve kterých se zaměstnanec nachází, jeho vztah k těmto prostorám, ale i dobu, kdy se zaměstnanec v těchto nachází.[39]

Demonstrovat toto lze na příkladu univerzitních pedagogů v případu Antović a Mirković v. Černá Hora.[40] Přednášková místnost, stejně tak jako jejich kancelář, jistě představuje jejich pracoviště. A přitom ve vztahu k instalaci kamer v přednáškové místnosti vnitrostátní soudy rozhodly ve prospěch univerzity – zaměstnavatele, když vyslovily názor, že přednášková místnost je veřejným prostorem a v takovém nelze hovořit o soukromí zaměstnance, a tedy potřebě jeho ochrany. Stěží si lze představit takovou argumentaci, jednalo-li by se o instalaci kamer do kanceláří pedagogů. Evropský soud pro lidská práva (dále jen „*ESLP*“) nicméně s uvedeným závěrem soudů nesouhlasil. Nelze však říct, že by o existenci soukromí zaměstnance v přednáškové místnosti a o neoprávněném zásahu do soukromí skrze kamerový systém rozhodl zcela jednoznačně – výsledné rozhodnutí bylo totiž přijato po hlasování čtyř soudců vůči třem. Ke konkrétní vybrané relevantní judikatuře ještě později, nyní zpět k obecné formulaci soukromí na pracovišti.

---

[37] NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 229, či MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, s. 58

[38] Obdobně viz PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 949

[39] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1242

[40] Rozhodnutí Evropského soudu pro lidská práva ve věci Antović a Mirković v. Černá Hora ze dne 28. 11. 2017 (konečné znění ze dne 28. 2. 2018), stížnost č. 70838/13

F. Nonnemann definuje soukromí jako „*osobní sféru každého člověka, která zahrnuje projevy osobnosti jedinečné lidské bytosti, její tělesnou i duševní integritu, alespoň některé hmotné statky i myšlenkový a názorový prostor, a to včetně možnosti rozvíjet vztahy s ostatními*.“[41] Kolektiv autorů v komentáři k ZP se pak v tomto názoru s výše uvedeným autorem v zásadě shoduje, když shrnuje, že soukromím se rozumí jak osobní soukromí člověka (tedy např. údaje identifikující jej), tak i právo každého člověka na vytváření a rozvíjení vztahů s dalšími, tedy jak soukromé, tak i profesní povahy, souhrnně interakce s ostatními zaměstnanci.[42] Literaturou často citovaným rozsudkem je pak Niemietz v. Německo[43], resp. následující vyjádření soudu z tohoto rozsudku: „*Respektování soukromého života musí do určité míry zahrnovat právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi*“.

Takové je tedy obecně řečeno základní vymezení pojmu soukromí zaměstnance, a to tedy bezpochyby existuje i na pracovišti. K čemuž lze na základě výše uvedeného dojít jak logickou úvahou, tak nahlédnutím do judikatury – poměrně široký výklad (a zároveň potvrzující existenci) soukromí zaměstnance na pracovišti lze nalézt i v dalších rozhodnutích ESLP, kdy např. v rozhodnutí ve věci Halford v. Velká Británie[44], ESLP shledal, že již výše zmíněný čl. 8 EÚLP se vztahuje, a jako do soukromí do něj nelze neoprávněně zasahovat, i na pracovní telefon zaměstnance. Tento názor ve vztahu k přesahu soukromí na pracoviště a pracovním telefonům pak ESLP potvrdil v rozhodnutí Copland v. Velká Británie[45] a rozšířil jej dále na e-mailové zprávy a používání internetu.

Právo na ochranu soukromí na pracovišti tak dnes již výkladem spadá pod zákonný nárok zaměstnance na příznivé pracovní prostředí.[46]

---

[41] NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 229

[42] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1242

[43] Rozhodnutí ESLP ve věci Niemietz v. Německo ze dne 16. prosince 1992, stížnost č. 13710/88

[44] Rozhodnutí ESLP ve věci Halford v. Velká Británie ze dne 26. června 1997, stížnost č. 20605/92

[45] Rozhodnutí ESLP ve věci Copland v. Velká Británie ze dne 3. 4. 2007 (konečné znění ze dne 3. 7. 2007), stížnost č. 62617/00.

[46] MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, s. 66

2.3.2. Zákoník práce

Nyní tedy k právní úpravě v samotných lex specialis (ve vztahu k problematice monitoringu zaměstnanců). Klíčovým je § 316 ZP. Úprava v tomto ustanovení se vztahuje na všechny zaměstnance, tedy nezáleží, zdali vykonávají práci na základě pracovní smlouvy či dohod o pracích konaných mimo pracovní poměr, a vůbec je potřeba ustanovení vykládat extenzivně.[47]

Jak již bylo zmíněno v úvodu práce, s rozvojem technologií si nejen zákonodárci uvědomují potřebu zakotvit ochranu soukromí skrze zákonná pravidla. Legislativa nutně musela na nastalou situaci zareagovat. Ještě v roce 2005 literatura kritizovala chybějící speciální, a tedy naprosto nedostatečnou úpravu v rámci pracovního práva,[48] (zřejmě) i proto byla v rámci přijetí nového zákoníku práce v roce 2006 do § 316 zakotvená pravidla pro ochranu majetkových zájmů zaměstnavatelů a ochrana osobních práv zaměstnanců. Alespoň tak lze chápat zdůvodnění nové úpravy z důvodové zprávy k příslušné novele: *„Nedostatek této úpravy se musí dohánět výkladem za použití obecných ústavních východisek vyplývajících z Listiny základních práv a svobod a za použití § 7 odst. 2 dosavadního zákoníku práce o postupu podle zásady dobrých mravů.“* [49]

Ve zmíněném § 316 ZP v jeho odst. 1) je tedy pravidlo o využívání pracovní doby blíže rozvedeno s doplněním oprávnění zaměstnavatele přiměřeně kontrolovat dodržování této povinnosti, ba dokonce formulované jako zákaz využívaní prostředků zaměstnavatele k užívání pro osobní potřebu. V následujícím odstavci, v § 316 odst. 2) ZP je stanoveno pravidlo o tom, že zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti narušovat soukromí zaměstnance a otevřeně, či skrytě jej sledovat, odposlouchávat, zaznamenávat jeho telefonické hovory a kontrolovat elektronickou či běžnou poštu zaměstnance.

[47] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 944

[48] ŠTEFKO, M. K problému sledování vlastních zaměstnanců. *Právo a zaměstnání*. 2015, **11**(1), s. 7, nebo např. BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016, s. 130

[49] Důvodová zpráva k návrhu ZP, sněm. tisk 1153/0, ze 4. období Poslanecké sněmovny (2002 – 2006)

Existuje-li však závažný důvod, zaměstnavatel smí zavést kontrolní mechanismy, zaměstnance je však potřeba předem informovat o rozsahu a způsobech takové kontroly.

Jak upozorňuje literatura, důležité je toto ustanovení především proto, že se od něj s ohledem na znění § 4b ZP nelze odchýlit ani se souhlasem stran. Proto i kdyby jinak daný způsob zpracování osobních údajů byl podle ZOOÚ možný se souhlasem subjektu údajů, je možné, že ZP jej nedovoluje a souhlas zaměstnance nelegálnost nenapraví.[50] Na což názorově navazuje další autor: „*Před posuzováním účelu zpracování v kontextu zákona o ochraně osobních údajů je třeba, aby byly naplněny ještě předpoklady podle § 316 odst. 1 až 3 ZPr.*“[51]

2.3.3. Zákon o inspekci práce

Výše přiblížená úprava v ZP dbá na ochranu zaměstnanců stanovením limitů pro zaměstnavatele pro výkon kontroly a monitoringu. V návaznosti na to jsou zaměstnanci chráněni de facto také úpravou v zákoně č. 251/2005 Sb., o inspekci práce, ve znění pozdějších předpisů (dále jen „*ZIP*“), který jim dává možnost bránit se proti neoprávněným zásahům skrze kontrolu ze strany inspektorátu práce. ZIP po nedávné novele s účinností od 29. 7. 2017 obsahuje dvě nová ustanovení.[52] Příslušné § 11a a § 24a ZIP obsahují nové přestupky resp. správní delikty zaměstnavatelů na úseku ochrany soukromí a osobních práv zaměstnanců. Podle těchto ustanovení je při porušení § 316 odst. 2) a odst. 4) ZP možno uložit pokutu až do výše 1.000.000 Kč. Za porušení § 316 odst. 3) ZP, tedy porušení informační povinnosti, pak pokutu až do výše 100.000 Kč. Při pohledu do literatury lze uzavřít, že až se zavedením těchto oprávnění pro inspektoráty práce se úprava ochrany

[50] RADIČOVÁ, Z. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy.* 2014 **22(**21), s. 736

[51] MORÁVEK, J. Sledování zaměstnanců v kontextu novely zákoníku práce. *Právní rozhledy.* 2012, **20**(5), s. 175

[52] Provedeno novelou ZIP publikovanou pod č. 206/2017 Sb.

soukromí zaměstnanců stala konečně efektivní a reálnou, nikoliv pouze proklamativní.[53]

3. Právo vlastnit majetek, ochrana majetku

Nyní k obecnému právnímu rámci ochrany majetku a speciální ochraně majetku zaměstnavatele.

3.1. Prameny mezinárodního práva

Stejně jako právo na ochranu soukromí, tak i právo vlastnit majetek a právo na ochranu majetku má svůj mezinárodněprávní (a ústavněprávní základ). Čl. 17 Listiny základních práv Evropské unie stanoví právo každého vlastnit zákonně nabytý majetek, užívat jej a nakládat s ním. Následující čl. 52 Listiny základních práv Evropské unie pak stanoví zásadu proporcionality při omezení výkonu práva. Omezení smí být zavedena pouze tehdy, pokud jsou nezbytná a odpovídají např. potřebě ochrany práv druhých.

Dodatkový protokol č. 1 k EÚLP stanoví ochranu majetku ve svém čl. 1.

3.2. Vnitrostátní právní úprava

3.2.1. Listina

V rámci vnitrostátního práva je pak na ústavní úrovni právo na vlastnictví a jeho ochranu zakotveno v čl. 11 odst. 1) Listiny, podle kterého má každý právo vlastnit majetek, a dále má vlastnické právo všech vlastníků stejný zákonný obsah a ochranu. Vlastník věci má právo ji užívat, disponovat s ní a rozhodovat o ní.

[53] BÁRTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1. 8. 2012*. 1. vydání. Olomouc: ANAG, 2012, s. 262

Vlastnictví pak působí vůči všem ostatním, kteří jsou povinni do vlastnictví bezdůvodně nezasahovat.[54]

Ve vztahu k majetku zaměstnavatele pak literatura došla k tomu, že zaměstnanec nesmí tento majetek užívat pro svoje soukromé účely, a to i bez existence explicitního zákazu zaměstnavatele.[55] Pokud tak zaměstnanec učiní, dopouští se tím porušení pracovních povinností a získá-li skrze toto jednání užitek, je povinen jej svému zaměstnavateli vydat.[56]

3.2.2. Občanské právo

Obecná úprava ochrany majetku, které se lze dovolávat např. v mezích občanského práva, není pro potřeby této práce zkoumat oprávnění zavést monitoring zaměstnanců na ochranu majetku zaměstnavatele nijak zvlášť relevantní, a proto se jí, na rozdíl od obecné úpravy práva na soukromí zaměstnance, jakožto člověka, tato práce blíže nevěnuje.

3.3. Ochrana majetku zaměstnavatele

Ačkoliv se tato část zaobírá prameny práva na ochranu majetku zaměstnavatele, začne nejdříve vlastně povinnostmi zaměstnance, které tomuto právu zaměstnavatele odpovídají a jejichž účelem je nepochybně chránit majetek zaměstnavatele.

3.3.1. Povinnost používat majetek k pracovním účelům

První z nich je povinnost zaměstnance používat svěřený majetek zaměstnavatele k pracovním účelům. Tato je výslovně (skrze zákaz použití pro osobní účely) zakotvena v první větě § 316 odst. 1) ZP. V tomto ohledu literatura

[54] WAGNEROVÁ, E., ŠIMÍČEK, V. a kol. *Listina základních práv a svobod: komentář*. 1. vydání. Praha: Wolters Kluwer ČR, 2012, s. 301

[55] MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013. s. 68, nebo VALENTOVÁ, K. Jak legálně sledovat zaměstnance. *Právní rádce*. 2016, **23**(7-8), s. 52

[56] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1242

kritizuje nepřesnou dikci tohoto ustanovení, neboť zaměstnanci bez souhlasu zaměstnavatele nemohou pro svou potřebu používat pouze majetek ve vlastnictví zaměstnavatele, ale taktéž majetek, který si zaměstnavatel může pronajímat apod. Tato povinnost by tedy měla platit ve vztahu k veškerému majetku, který nepatří zaměstnanci.[57]

Protože je zákaz používání výrobních a pracovních prostředků zaměstnavatele k osobním účelům zaměstnance zakotven již v zákonné úpravě, nemusí jej zaměstnavatel dále zahrnout do vnitřních předpisů či pracovních smluv, aby jím byli zaměstnanci vázáni a byli povinni jej dodržovat.[58]

I samotné označení výrobních a pracovních prostředků literatura kritizuje. Jedná se o příliš úzké vymezení, neboť pod tento zákaz zneužívání prostředků zaměstnavatele jistě spadají i služby placené zaměstnavatelem (např. datové připojení) atp.[59]

Dále podle § 301 písm. b) ZP jsou zaměstnanci povinni využívat pracovní dobu a výrobní prostředky k vykonávání svěřené práce a podle § 301 písm. d) ZP pak řádně hospodařit s prostředky svěřenými jim zaměstnavatelem a střežit a ochraňovat majetek zaměstnavatele, mj. před zneužitím a nejednat v rozporu s oprávněnými zájmy jejich zaměstnavatele. V § 301 písm. c) ZP je pak stanovená obecná povinnost dodržovat právní předpisy vztahující se k jimi vykonávané práci a taktéž ostatní předpisy, se kterými je zaměstnavatel řádně seznámil. Mezi tyto se nepochybně řadí pravidla výše jmenovaná a dále případně vnitřní předpisy zaměstnavatele upravující tuto povinnost blíže.

V návaznosti na toto jsou vedoucí zaměstnanci podle § 302 ZP povinni řídit a kontrolovat práci svých podřízených a mimo jiné také zabezpečovat přijetí opatření k ochraně majetku zaměstnavatele.

---

[57] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 945.

[58] BÁRTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1. 8. 2012*. 1. vydání. Olomouc: ANAG, 2012, s. 258

[59] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 945

Již z tohoto tedy lze vyvodit povinnost zaměstnance věnovat se v pracovní době pracovním úkolům, a nikoliv vyřizování soukromých záležitostí. V tomto ohledu nehraje významnou roli, zdali hrozí, že by byla zaměstnavateli takovým jednáním způsobená škoda. Pomineme-li výplatu mzdy za dobu, kdy zaměstnanec fakticky práci nevykonává, pak se zákaz používání zaměstnavatelových prostředků vztahuje i na případy, kdy si například zaměstnanec na pracovním telefonu s neomezeným limitem volání vyřizuje soukromou záležitost (bez souhlasu zaměstnavatele). Takové situace proto představují bezdůvodné obohacování zaměstnance.[60]

K povinnosti zaměstnance využívat pracovní dobu pro výkon práce a používání telefonů v rámci pracovní doby se váže stanovisko Asociace kolektivního vyjednávání (dále jen „*AKV*“), které se zaobíralo používáním soukromých telefonů namísto výkonu práce v pracovní době.[61] Dotazy položené AKV směřovaly na možnost zakázat zaměstnancům používání vlastních mobilních telefonů (s různými variacemi pro zaměstnance, kteří jsou zároveň rodiči atp.). AKV na tyto otázky odpovědělo tak, že absolutní zákaz nošení mobilních telefonů na pracoviště je příliš přísný a případné odůvodnění by muselo odpovídat závažnosti (jako příklad uvedena ochrana před průmyslovou špionáží). Vzhledem k tomu, že tedy fakticky spíše neexistuje možnost, jak vlastní telefony zaměstnancům na pracovištích zakázat, navrhlo AKV řešení k jednomu z dotazů, že nedodržování povinnosti výkonu práce v pracovní době může být postihováno jako porušování povinností (dle starší terminologie „pracovní kázně“), které tedy může vést až k ukončení pracovního poměru, popř. mělo-li by nadměrné používání telefonu vliv na pracovní výsledky zaměstnance a jeho kvalitu práce, pak lze uvažovat i o nepřiznání prémiové (nenárokové) složky mzdy. V této záležitosti lze spatřit silný prvek ochrany soukromí zaměstnance, kdy jej lze přimět k dodržování povinností nepřímo, skrze sankce výtek a nepřiznání bonusů.

[60] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 946.

[61] Výkladová stanoviska AKV (XIX.), přijatá na zasedání Kolegia expertů AKV v Kolíně ve dnech 4. a 5. 11. 2016 – IV. část, část 24.

Nicméně zpět k věcem, které patří zaměstnavateli. Zaměstnavatel logicky může zaměstnancům dovolit, aby jeho majetek a tyto svěřené prostředky používali taktéž k osobním účelům. S ohledem na to, že tento souhlas nemá stanovenou formu, může jej zaměstnavatel udělit konkludentně, a to prostým tolerováním takového chování.[62] V takovém případě není zaměstnavatel oprávněn vyžadovat důsledné plnění povinností zaměstnance používat jím svěřený majetek pouze k pracovním účelům, dokud tuto svou politiku nezmění a zaměstnance o tom nevyrozumí. Dále literatura vysvětluje, že co do rozsahu možnosti povolit zaměstnancům využití prostředků i k jiným, než pracovním účelům zaměstnavatel omezen není, co do rozsahu možnosti výkonu kontroly tohoto užití už ovšem ano – a to s odkazem na § 316 odst. 1) ZP větu druhou.[63][64]

3.3.2. Povinnost zaměstnance odvrátit škodu

Vhodné je také v krátkosti zmínit zaměstnancovu prevenční povinnost škodám předcházet a povinnost škody odvracet. Zmíněné lze nalézt v § 249 ZP, dle kterého jednání zaměstnance nesmí vést ke vzniku škody, nemajetkové újmy, ani k bezdůvodnému obohacení. Nebrání-li v tom zaměstnanci okolnosti a neohrožuje-li to jeho nebo osobu jemu blízkou, je povinen zakročit v případě hrozícího nebezpečí a zabránit tomu, aby ke škodě došlo.

3.4. Právo na ochranu majetku zaměstnavatele

Nyní tedy k samotným explicitním právům zaměstnavatele chránit svůj majetek. Krom již zmíněného § 316 ZP, který tedy obsahuje jak pravidla ochrany soukromí zaměstnance, tak právo zaměstnavatele zabezpečit svůj majetek prováděním kontrol, lze dále nalézt právo zaměstnavatele chránit svůj majetek skrze kontrolu vnášených a odnášených věcí zaměstnanci v § 248 odst. 2) ZP.

[62] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 946

[63] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 947

[64] Viz také např. rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1771/2011, k tomuto blíže viz kapitola 4.3.3.

Zaměstnavatel je v tomto omezen co do rozsahu kontroly, která má být provedena jen v míře nezbytné, dále musí být při prohlídce dodržena ochrana osobnosti[65] a osobní prohlídku může provést jen osoba stejného pohlaví. Výkon kontroly musí probíhat v souladu s dobrými mravy a dále literatura rozvádí, že by měl zaměstnavatel ke kontrolám přistoupit až v případě (důvodného) podezření, že k odcizování věcí dochází.[66]

Dle literatury je možnost vykonávat kontrolu užívání majetku zcela legitimní a logická. Kdyby tuto možnost zaměstnavatel právem dovolenou neměl, došlo by tak až k popření ústavně zaručeného práva vlastnictví.[67]

Výkon kontroly lze označit za část výkonu práva na ochranu majetku, dalším důležitým důsledkem, zjistí-li zaměstnavatel, že zaměstnanec zneužívá jemu svěřený majetek zaměstnavatele k osobním účelům, je možnost postihnout zaměstnance tak, aby se podobné zneužívání v budoucnu neopakovalo a zaměstnavatelův majetek tak byl chráněn. V tomto smyslu je potřeba zhodnotit míru zneužití zaměstnavatelova majetku a s ohledem na toto pak vyhodnotit, zda se zaměstnanec dopustil méně závažného, či závažného porušení svých povinností vyplývajících mu z právních předpisů vztahujících se k výkonu jeho práce a přistoupit od postihu vytýkacího dopisu až k ukončení pracovního poměru, a to s odkazem na § 52 písm. g) ZP. V tomto směru nelze ani vyloučit okamžité zrušení pracovního poměru podle § 55 ZP.[68]

[65] Literatura v tomto směru odkazuje, zřejmě na základě principu subsidiarity, na již dříve zmíněnou úpravu v § 81 an. ObčZ. Viz BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1018

[66] ANDRAŠČÍKOVÁ, M., HLOUŠKOVÁ, P. a kol. *Zákoník práce: prováděcí nařízení vlády a další související předpisy: s komentářem k 1. 1. 2016*, s. 390

[67] MORÁVEK, J. Sledování zaměstnanců v kontextu novely zákoníku práce. *Právní rozhledy.* 2012, **20**(5), s. 176

[68] MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, s. 405.

4. Monitoring zaměstnanců

Nyní již konkrétně k samotnému monitoringu zaměstnanců. Krom rozdělení na jednotlivé konkrétní formy monitoringu lze monitoring zaměstnanců dělit např. na nahodilý a soustavný. Nahodilý, nebo také *ad hoc,* monitoring je upraven v § 316 odst. 1) ZP, soustavný je pak upraven v § 316 odst. 2) ZP.[69]

Ustanovení § 316 odst. 2) a 3) ZP stanoví omezení zaměstnavatele ve vztahu k systematickému monitoringu. V tomto ohledu se vede diskuze ohledně ne příliš jasného vyslovení podmínky spočívající ve zvláštní povaze činnosti zaměstnavatele, pro kterou je možno soustavný monitoring zavést. Lze nalézt názor, že záměrem zákonodárce bylo cílit na specifické zaměstnavatele, u nichž je třeba dbát zvýšených nároků na chování zaměstnanců (a to např. s ohledem na ochranu utajovaných skutečností, vyšších majetkových hodnot či know how atd.),[70] nebo jsou za takové specifické činnosti označovány mezinárodní bankovní převody či dozor nad prací vězňů.[71] Na druhou stranu je ovšem také možné se dočíst, že při splnění ostatních zákonných podmínek má právo zavést soustavný monitoring každý zaměstnavatel[72], tedy nejen tito bezpochyby specifičtí zaměstnavatelé naznačeni literaturou výše. Nicméně dlužno ještě dodat k tomuto dělení – nelze uzavřít, že by s tímto všichni autoři souhlasili. Lze se dočíst, že celý § 316 ZP upravuje monitoring soustavný, a to s odkazem na znění ustanovení, které podle autora volí slova významově indikující soustavnost monitoringu.[73] Je otázkou, zda taková interpretace nevytváří nepravou mezeru v právu. Lze se případně domnívat, že autor tím měl na mysli situace, kdy kontrola není prováděna ani za účelem sledování plnění pracovních povinností zaměstnance

[69] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 947 – 948.

[70] BÁRTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1. 8. 2012*. 1. vydání. Olomouc: ANAG, 2012, s. 259

[71] Stanovisko ÚOOÚ č. 2/2009

[72] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1243.

[73] NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 233

ani využívání svěřených prostředků, v takovém případě se totiž aplikuje pouze ZOOÚ z titulu zpracování osobních údajů.[74]

Dále je možné rozlišovat monitoring otevřený a skrytý. Z pohledu přípustnosti obou nepanuje v literatuře shoda. Na jedné straně existují názory, že zaměstnavatel je oprávněn provádět sledování pouze otevřenou formou,[75] na druhou stranu se lze dočíst, že zákon upravuje i sledování skryté, tedy takové by za dodržení ostatních podmínek mělo být přípustné.[76][77] Každopádně takové by mělo být prováděno skutečně výjimečně.[78]

Předtím než přejdeme k jednotlivým formám monitoringu, je potřeba prozkoumat obecně na úvod zákonné důvody umožňující monitoring provádět a dále povinnosti, které jsou se sledováním a kontrolou zaměstnanců spojené. S ohledem na konkrétní volbu způsobu monitoringu je potřeba určit vybraný relevantní legitimní důvod, jinými slovy, bude-li u zaměstnavatele existovat relevantní, zákonem předpokládaný důvod, bude tento oprávněn monitoring zaměstnanců na pracovišti zavést a provádět.[79] Existence zákonného a legitimního důvodu je označována za nejdůležitější

[74] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 953

[75] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1244.

[76] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 948

[77] Nad rámec tohoto, ale z důvodu zajímavosti a vztahu k tématu, bych zde ráda stručně zmínila rozhodnutí Ústavního soudu II. ÚS 1774/14 ze dne 9. 12. 2014, které diskutovalo přípustnost skrytého sledování. Tam, kde by skryté sledování zaměstnance ze strany zaměstnavatele bylo naprosto nepřípustné, Ústavní soud v soudním sporu povolil jako důkaz skrytě pořízenou nahrávku kolegy zaměstnance, který byl propuštěn, neboť tento rozhovor poskytoval jasný důkaz, že tvrzená nadbytečnost propuštěného zaměstnance byla zcela vykonstruovaná. Skrytý monitoring, ovšem prováděný zaměstnancovým spolupracovníkem, byl označen jako přípustný. Toto rozhodnutí opět dokazuje, jak je vždy potřeba hodnotit danou situaci a postavení sledujících, kdy zaměstnanci mohou být v pracovní m sporu co do rozsahu důkazních prostředků v nevýhodě.

[78] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 952

[79] BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer ČR, 2016, s. 131

náležitost sledování zaměstnanců.[80] Zvolená forma kontroly se pak promítne do konkrétního rozsahu povinností souvisejících se zavedením a prováděním kontroly.

Konečně co do dopadu aplikace § 316 ZP, právo výkonu kontroly (opět při splnění všech podmínek), svědčí zaměstnavateli jak na pracovišti zaměstnance, tak i mimo tyto prostory a jak v pracovní době, tak případně i mimo ni.[81] Nicméně s výhradou určitých prostor, kde monitoring zkrátka nebude přípustný nikdy (např. sprchy, toalety apod.).[82]

4.1. Legitimní důvody – stanovení účelu monitoringu

ZP tedy umožňuje zavést monitoring z důvodu kontroly užívání pracovních prostředků ke stanoveným účelům. Při monitoringu však může docházet ke zpracování osobních údajů zaměstnanců. Proto je, jak již bylo výše zmíněno, relevantní nejen úprava v ZP, ale také v ZOOÚ. Vedle důvodů pro zavedení monitoringu podle § 316 odst. 3) ZP stanoví ZOOÚ taxativní výčet legitimních důvodů. Prvním z těchto titulů je souhlas subjektu – podle § 5 odst. 2) ZOOÚ mohou být osobní údaje subjektů zpracovávány pouze s jejich souhlasem, dle textace zákona výjimky z tohoto pravidla přináší následující část § 5 odst. 2) písm. a) – g) ZOOÚ.

Správně a dostatečně stanovit účel monitoringu není důležité pouze proto, aby sledování zaměstnanců probíhalo v souladu se zákonem, ale i ve vztahu k následné možnosti nakládat s údaji či informacemi pořízenými skrze toto sledování. Tyto totiž smějí být použity pouze v souladu s deklarovaným účelem,

[80] NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 233, či obdobně TOMŠEJ, J., METELKA, J. *Ochrana soukromí nad zlato.* Server https://www.epravo.cz. Dostupné online na WWW <https://www.epravo.cz/top/clanky/ochrana-soukromi-nad-zlato-92358.html> [cit. 29.4.2018]

[81] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 949

[82] Tamtéž, s. 952

jinak se jedná o porušení zákona, podle literatury dokonce jedno z nejčastějších porušení ZOOÚ.[83]

4.1.1. Zpracování se souhlasem zaměstnance

Požádat zaměstnance o souhlas pro provádění monitoringu není příliš praktické řešení. Zaměstnavatel jej totiž musí být schopen prokázat po celou dobu zpracování osobních údajů[84] a zaměstnanec jej z logiky věci může vzít kdykoliv zpět. Navíc se lze setkat s názorem, že z důvodu existence speciální úpravy v ZP nelze použití souhlasu jako právní úpravou uznaného důvodu ke zpracování osobních údajů vzít vůbec v úvahu.[85] Jiní autoři jsou stejného názoru, argumentem pak je, že právo na soukromí a ochranu osobnosti se řadí mezi základní lidská práva a tyto jsou ze své podstaty nezadatelná, nezcizitelná, nepromlčitelná a nezrušitelná. Nelze tedy dojít k závěru, že se těchto lze zbavit, byť vlastním souhlasem, autoři navíc připomínají úpravu v tehdejším znění § 19 ZP (pozn. v současnosti obdobně upraveno v § 4a ZP), podle kterého se zaměstnanec nemůže platně předem vzdát svých práv.[86] Komentářová literatura k tomuto uvádí, že za platný souhlas zaměstnance k omezení soukromí lze považovat pouze situaci, kdy by v případě neudělení souhlasu zaměstnanci nehrozily žádné následné postihy.[87]

K problematice souhlasu se lze dále taktéž dočíst, že je v pracovněprávním vztahu vůbec problematická otázka, na kolik jej zaměstnanec dává svobodně, kdy svoboda při udílení souhlasu je jeden ze základních atributů, a jestli se zaměstnanec skutečně může svobodně rozhodnout souhlas neudělit, aniž by mu hrozily jakékoliv

[83] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců.* 1. vydání. Praha: C.H. Beck, 2013, s. 169

[84] Stanovisko ÚOOÚ č. 3/2014

[85] MORÁVEK, J. Sledování zaměstnanců v kontextu novely zákoníku práce. *Právní rozhledy.* 2012, **20**(5) s. 175.

[86] BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer ČR, 2016, s. 131

[87] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1243

negativní následky.[88] Ani tzv. pracovní skupina 29 (dále jen „*Skupina WP29*“)[89] není toho názoru, že by s ohledem na nerovnováhu vztahu zaměstnavatel - zaměstnanec mohl zaměstnanec nějaký svobodný souhlas dát.[90] V souladu s výše uvedeným se lze tedy v literatuře dočíst, že takový souhlasu je buďto nadbytečný (zaměstnavatel naplňuje podmínky podle ZP), nebo zbytečný (zaměstnavatel tyto nesplňuje a souhlas pak nezákonnost monitoringu nezhojí).[91]

4.1.2. Zpracování bez souhlasu zaměstnanců

Zaměstnavatelé proto spíše než souhlas zaměstnanců využijí ony „výjimečné“ možnosti zpracování osobních údajů svých zaměstnanců (v rámci monitoringu) bez zisku jejich souhlasu zmíněné v úvodu této podkapitoly výše.

Pohledem do zmíněné úpravy § 5 odst. 2) písm. a) – g) ZOOÚ se pro potřeby zavedení a provádění monitoringu nabízí možné využití zejména následujících důvodů:

i. jestliže je zpracování nezbytné pro dodržení právní povinnosti správce,[92]

ii. jestliže je zpracování nezbytné pro plnění smlouvy, v tomto případě pracovní smlouvy,[93]

iii. je-li zpracování nezbytné pro ochranu práv a právem chráněným zájmů správce.[94][95]

---

[88] NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 235

[89] Označení pro Pracovní skupinu pro ochranu údajů zřízenou podle článku 29 Směrnice. Jedná se o poradní orgán Evropské komise.

[90] Stanovisko Skupiny WP29 č. 2/2017, str. 4, dostupné online na WWW <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169>, [cit. 1.4.2018]

[91] VALENTOVÁ, K. Jak legálně sledovat zaměstnance. *Právní rádce*. 2016, **23**(7-8), s. 54

[92] Viz § 5 odst. 2) písm. a) ZOOÚ. Jedná se tedy o povinnosti vzniklé přímo ze zákona, podzákonných právních předpisů, případně uložené rozhodnutím orgánu veřejné moci, viz MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, s. 265.

[93] § 5 odst. 2) písm. b) ZOOÚ

[94] § 5 odst. 2) písm. e) ZOOÚ

[95] Literatura jako příklad uvádí kamerový systém chránící sklad zaměstnavatele či vstupy do objektu. Viz NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 235

Nicméně je třeba podotknout, že jedna úprava druhou nevylučuje. Naopak, před posouzením účelu pro zpracování údajů subjektů v kontextu ZOOÚ je potřeba, aby byly naplněny předpoklady podle § 316 ZP.[96] Právní úprava v ZP tedy „*stanoví dodatečné podmínky, které zaměstnavatel musí naplnit před zavedením sledovacích opatření*.“[97]

Jako konkrétní důvody pak literatura uvádí, vedle již zmíněné ochrany majetku zaměstnavatele, také ochranu majetku spoluzaměstnanců, ochranu života a zdraví zaměstnavatele i zaměstnanců, ale i jiných osob, které se v kontrolovaném prostoru vyskytují a kontrolu pracovní výkonnosti zaměstnanců provádějí.[9899] Poslední jmenovaný důvod vyplývá z výše uvedené možnosti kontrolovat využívání pracovní doby k plnění pracovních úkolů za pomoci pracovních prostředků ve vlastnictví zaměstnavatele.

Obecně lze také dále říct, že naplnění zákonných podmínek není důležité jen při zavádění monitoringu, ale po celou dobu provádění sledování zaměstnanců,[100] a proto je potřeba jejich splňování průběžně sledovat.

Poslední poznámka k zákonným titulům bude věnována výhledu do blízké budoucnosti – tato pravidla se totiž ani po nabytí účinnosti GDPR nezmění. Právní úprava v ZP jakožto lex specialis bude i nadále relevantní a platná a dále lze při pohledu do článku 6 GDPR uzavřít, že výše zmíněné tituly pro zpracování údajů, které v současnosti nabízí ZOOÚ, zůstanou zachovány.

---

[96] MORÁVEK, J. Sledování zaměstnanců v kontextu novely zákoníku práce. *Právní rozhledy.* 2012, **20**(5), s. 175

[97] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1242

[98] Tamtéž, s. 1243

[99] Velice obdobně lze nalézt uvedené důvody opravňující zaměstnavatele zavést a provádět sledování zaměstnanců (byť vyjmenované ve vztahu ke kontrole elektronické pošty) např. v JOUZA, L. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. *Bulletin advokacie*. 2014, **21**(6), s. 28

[100] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 953

4.2. Povinnosti zaměstnavatele spojené s monitoringem

Povinnosti zaměstnavateli v této souvislosti stanoví jak úprava v ZP, tak v ZOOÚ. Úprava v ZOOÚ se na zaměstnavatele bude vztahovat vždy, bude-li docházet ke zpracování osobních údajů zaměstnanců v rámci monitoringu. Hovoříme o takovém monitorovacím systému, který uchovává záznam pořízených záběrů či informací a zároveň je účelem takto pořízeného záznamu identifikace jednotlivých osob. Co se týče doby uchovávání záznamů, pak dlouhodobě by měly být uchovávány pouze ty záznamy, které prokazují, že se zaměstnanec dopustil porušení pracovních povinností.[101]

4.2.1. Zásada proporcionality

První povinností, či spíše omezením, které musí zaměstnavatel respektovat, je omezení zásadou přiměřenosti. Způsob, jakým se zaměstnavatel rozhodne monitorovat své zaměstnance, musí být vhodný, nutný a přiměřený.[102] Zaměstnavatel tedy ještě před zavedením monitoringu musí prozkoumat a zvážit, zda jím zamýšlená forma kontroly nezasahuje do zaměstnancova práva na soukromí nad míru přijatelnou a přípustnou a zda nelze použít jinou, méně invazivní formu monitoringu, která by plnila zvolený účel ochrany stejně tak. Při monitoringu totiž dochází ke kolizi dvou základních práv, jak již bylo zmíněno v úvodu a do těchto lze zasáhnout pouze tehdy, splní-li řešení test proporcionality. Tato zásada je de facto zakotvena hned v několika předpisech[103] a pravidelně se objevuje také v soudních rozhodnutích, včetně těch od soudu Ústavního.[104]

[101] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1243 – 1244

[102] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 947

[103] Dále se text věnuje pouze vnitrostátním předpisům, co se týče mezinárodní úrovni, pak již byl výše zmíněn čl. 52 Listiny základních práv Evropské unie.

[104] Viz např. nález Ústavního soud Pl. ÚS 4/94 ze dne 12. 10. 1994, publikováno pod č. 214/1994 Sb., nebo také nález Ústavního soudu Pl. ÚS. 3/02 ze dne 13. 8. 2002, publikováno pod č. 405/2002 Sb.

Na ústavní úrovni je zásada proporcionality zachycena v čl. 4 odst. 4 Listiny, který stanoví, že „*při používání ustanovení o mezích základních práv a svobod musí být šetřeno jejich podstaty a smyslu. Taková omezení nesmějí být zneužívána k jiným účelům, než pro které byla stanovena*."

Toto omezení je dále vyjádřeno přímo v samotném ustanovení opravňujícím zaměstnavatele kontrolu zaměstnanců provádět, a to sice v textaci druhé věty § 316 odst. 1) ZP, které zaměstnavateli dovoluje kontrolu provádět, toliko však pouze přiměřeným způsobem.

Konečně toto omezení stanoví i úprava obsažená v ZOOÚ, kdy lze uzavřít, že dikce § 5 odst. 1 písm. d) a § 10 ZOOÚ vyjadřuje prakticky totéž.[105] Tedy že zpracování údajů subjektů lze provádět a zásah do soukromí respektovat jen v nezbytném, přiměřeném rozsahu a dále je při něm třeba dbát na zachování lidské důstojnosti a ochranu před neoprávněným zásahem do osobního života subjektu.

ÚOOÚ v tomto směru dodává, že zásada přiměřenosti se netýká jen obecně posouzení formy monitoringu, ale také rozsahu zpracovávaných osobních údajů zaměstnanců. Označuje speciálně tuto zásadu jako *zásadu adekvátnosti*. Zaměstnavatel je podle této povinen zpracovávat co nejmenší počet shromažďovaných osobních údajů výlučně kategorií odpovídajících účelu monitoringu.[106]

Literatura k tomuto dodává, že co se týče kontroly výkonnosti zaměstnance, pak je tato primárně povinností příslušného vedoucího zaměstnance.[107] Nicméně i tak může být kontrola výkonnosti zaměstnance jedním z důvodů pro zavedení monitoringu, viz rozbor v části 4.1.2. výše.

[105] MORÁVEK, J. Sledování zaměstnanců v kontextu novely zákoníku práce. *Právní rozhledy.* 2012, **20**(5), s. 176

[106] Stanovisko ÚOOÚ č. 2/2009, s. 2

[107] Bělina, Beck, s BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1244

4.2.2. Informační povinnost

Otázce možnosti otevřeného a skrytého sledování byla věnována pozornost výše. K tomuto pouze jen informace, že v případě otevřeného sledování zaměstnavatel plní informační povinnost předem a v případě skrytého pak bezprostředně po výkonu kontroly.[108] Toto dělení již nadále nebude diskutováno a zaměříme se proto na rozbor samotného znění § 316 odst. 3) ZP.

Podle tohoto ustanovení jsou zaměstnavatelé zavádějící kontrolní mechanismy podle § 316 odst. 2) ZP povinni přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění. Pro zpracování osobních údajů je tato povinnost velice obdobně zakotvena v § 11 ZOOÚ,[109] ovšem pozor, informační povinnost podle ZOOÚ se nevztahuje pouze na zaměstnance zaměstnavatele, ale i na další subjekty osobních údajů, kteří se budou v monitorovaných prostorech nacházet.[110] Dále pak stojí za pozornost porovnání rozsahu informační povinnosti v obou úpravách, ta podle ZOOÚ je totiž širší, nežli informační povinnost podle ZP.[111] Zaměstnavatelé by měli na toto dbát a v případě aplikace obou úprav na danou situaci s ohledem na ZOOÚ poučovat zaměstnance nejen o způsobu a rozsahu kontroly, ale také o dalších náležitostech stanovených ve zmíněném § 11 ZOOÚ. Jednou z těchto dalších náležitostí je povinnost informovat o tom, pro jaký účel budou osobní údaje zpracovávány. Tuto svoji informační povinnost může zaměstnavatel splnit např. rozmístěním informativních cedulí a dále informovat skrze podrobný popis ve vnitřním předpise či v kolektivní smlouvě.[112]

I v souvislosti s informační povinností lze nalézt nejednotné výklady. Na jednu stranu podle některých informace směřovaná zaměstnancům musí být

[108] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 953

[109] Případně v §5/4 ZOOÚ, jedná-li se o zpracování se souhlasem subjektu.

[110] Stanovisko ÚOOÚ č. 2/2009

[111] NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 234

[112] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1244.

zásadně písemná[113] a na druhou stranu podle jiných postačí, je-li jakkoliv zprostředkována přímo monitorovanému zaměstnanci.[114] Samotné vydání a odkaz zaměstnance na příslušný vnitřní předpis pak podle názoru dalšího autora nestačí, zaměstnance je potřeba s tímto seznámit, předpis mu vybranou formou předat.[115]

Obsahem informace je pak především rozsah kontroly a způsob jejího provádění[116] a zmíněný účel. V případě, že se aplikuje i ZOOÚ, pak je informační povinnost rozšířena i dle tohoto zákona, jak bylo zmíněno výše.

4.2.3. Oznamovací (registrační) povinnost

V současné době je správce údajů povinen, a to s odkazem na § 16 ZOOÚ, písemně předem oznámit ÚOOÚ svůj záměr zpracovávat osobní údaje, nebo změnit registrované zpracování údajů. Zpracování údajů, na které se tato oznamovací povinnost nevztahuje, lze nalézt v § 18 ZOOÚ s tím, že z pohledu zaměstnavatele bude ze tří výjimek nejvýznamnější zřejmě ty uvedené v § 18 odst. 1) pod písm. b) ZOOÚ, a to sice ukládá-li jiný zákon povinnost údaje zpracovávat, nebo je-li potřeba zpracovávat osobní údaje k uplatnění práv a povinností vyplývajících ze zákona. Pokud se na zpracování vztahuje oznamovací povinnost, pak je podle § 19 ZOOÚ správce povinen oznámit taktéž ukončení zpracování a dále jak bylo naloženo se zpracovávanými údaji.

Podle komentáře je kontrola zaměstnanců podle § 316 ZP vždy fakultativním důvodem pro zpracování údajů zaměstnanců a zaměstnavatel je proto povinen tento svůj záměr ÚOOÚ vždy oznámit.[117] Tato výjimka tak tedy zřejmě nedopadá na zavedení monitoringu za účelem ochrany práv vyplývajících zaměstnavateli ze ZP. Nelze ji totiž vztáhnout na zpracování osobních údajů, které zaměstnavateli

[113] Tamtéž, s. 1244

[114] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 953

[115] NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 232

[116] Viz § 316 odst. 3) ZP

[117] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1024.

výslovně zvláštní zákon neukládá. Literatura proto jako příklad výjimky spadající pod § 18 odst. 1) písm. b) uvádí zpracování personální a mzdové agendy.[118]

Ve vztahu k monitoringu by pod tuto výjimku mohlo spadat zavedení kamerového systému se záznamem pouze tehdy, pokud by takové zavedení zaměstnavateli výslovně zvláštní zákon ukládal.[119]

V tomto kontextu je třeba dále podotknout, že výjimka z oznamovací povinnosti nezbavuje zaměstnavatele dalších povinností, které mu ukládá ZOOÚ při zpracovávání osobních údajů zaměstnanců.[120]

Nicméně k tomuto již vydal ÚOOÚ tiskovou zprávu, ve které informuje o tom, že po nabytí účinnosti GDPR již splnění této povinnost nebude vyžadováno.[121]

4.2.4. Povinnost zabezpečit osobní údaje

Konečně poslední důležitou povinností stanovenou zaměstnavateli při výkonu kontroly zaměstnanců je povinnost zabezpečit data – osobní údaje shromážděné při monitoringu. Konkrétně podle § 13 ZOOÚ nesmí dojít k neoprávněnému nebo nahodilému přístupu k těmto datům, data nesmějí být změněna, zničena, ztracena, neoprávněně přenesena, jinak neoprávněně zpracována či jakkoliv jinak zneužita. Dále je ve zmíněném § 13 ZOOÚ výčet rizikových oblastí, kterým by měl zaměstnavatel věnovat pozornost a přijmout příslušná technicko-organizační opatření. Zaměstnanci zaměstnavatele, kteří budou tato data zpracovávat, jsou pak v souladu s § 15 ZOOÚ vázaní povinností mlčenlivosti,

[118] MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, s. 345. Stejný názor zastává i ÚOOÚ viz stanovisko ÚOOÚ č. 6/2012, podle kterého zpracování mzdové a personální agendy nepodléhá oznamovací povinnosti.

[119] MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, s. 346

[120] Stanovisko ÚOOÚ č. 6/2012

[121] Tisková zpráva ÚOOÚ ze dne 1. 3. 2018: „S účinností GDPR končí oznamovací povinnost správců“, dostupná online na WWW <https://www.uoou.cz/s-nbsp-ucinnosti-gdpr-konci-oznamovaci-povinnost-spravcu/d-28855>, [cit. 10.4.2018]

což je s ohledem na zařazení ustanovení další ze způsobů, jak zabránit zneužití dat a zachovat jejich bezpečnost.

Zaměstnanci jsou podle § 301 písm. c) ZP povinni dodržovat právní předpisy vztahující se k jimi vykonávané práci, ovšem za předpokladu, že s těmito předpisy byli řádně seznámeni. Tedy informovat zaměstnance o povinnosti zachovávat mlčenlivost při zpracování dat získaných při monitoringu se dá označit za důležitou povinnost zaměstnavatele stanovenou za účelem zabezpečit osobní údaje.

4.3. Jednotlivé formy monitoringu

Nyní přistoupíme k jednotlivým formám monitoringu.

4.3.1. Kontrola e-mailové a obdobné elektronické korespondence

První konkrétní forma monitoringu, které bude věnována pozornost, se týká kontroly e-mailů, ale i dalších forem elektronické komunikace, mezi něž řadíme také různé aplikace a platformy, které se dnes vedle klasických e-mailů v zaměstnání používají, jako např. Facebook messenger, Yahoo messenger, Whatsapp atp. I na tyto se totiž vztahuje ústavní ochrana listovního tajemství.[122] Při sledování e-mailové a obdobné korespondence hraje významnou roli princip proporcionality, ale také důvodné očekávání soukromí zaměstnance. Nejnižší, resp. až žádné by měl zaměstnanec mít v případě, kdy spravuje datovou schránku zaměstnavatele.[123]

V relevantním stanovisku ÚOOÚ k ochraně soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště[124] lze nalézt výklad k povaze e-mailové korespondence.[125] E-mailová adresa sice patří zaměstnavateli, nicméně

[122] S odkazem na s. 2 stanoviska ÚOOÚ č. 2/2009: „*Nové informační technologie je vhodné připodobnit starým technologiím (např. poště) a právní normy je regulující používat obdobně*.“ Zaměstnavatelé jsou s ohledem na uvedené i vztahu k novým technologiím povinni respektovat ochranu listovního tajemství a důvěrnosti dopravovaných zpráv.

[123] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1245

[124] Stanovisko ÚOOÚ č. 2/2009

[125] Literatura ovšem upozorňuje na dobu vzniku, a proto na potřebný rezervovaný přístup pří práci se zmíněným stanoviskem ÚOOÚ č. 2/2009, viz BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1245

obsahuje-li jméno a příjmení zaměstnance, pak je zpráva na ni doručená považována za soukromou elektronickou poštu. Pakliže je e-mailová adresa složena bez použití těchto identifikátorů, tedy ve formě *info@doména.cz*, jedná se podle ÚOOÚ o úřední elektronickou adresu, a to i kdyby ji používal pouze jeden zaměstnanec.[126] Nicméně toto dělení má při posuzování legitimity monitoringu pouze dílčí význam a jedná se tak jen o jeden z více faktorů, ke kterým je třeba přihlížet. Dalším z nich je pak například oslovení v e-mailu atp.[127]

Co se týče monitoringu obsahu e-mailové korespondence zaměstnanců, ÚOOÚ v tomto stanovisku striktně deklaruje, že zaměstnavatel nesmí tento sledovat a zpracovávat tak obsah této korespondence.[128] S tímto autoři odborných publikací souhlasí a shodně dodávají, že pro výkon práva sledovat zaměstnance, jak dodržují pracovní dobu a její využití, má zaměstnavatel možnost sledovat pouze počet e-mailů přijatých a odeslaných[129] a dále ještě adresy odesílatele.[130] Stejnou informaci lze nalézt i v krátké tiskové zprávě Státního úřadu inspekce práce k monitoringu zaměstnanců.[131]

Důležitá je tedy povaha e-mailu. Aniž by tak zaměstnavatel musel e-mail otevírat, tak podle odesílatele, předmětu a případně oslovení příjemce lze povahu e-mailu odhadnout.[132] Obdobný závěr lze nalézt ve stanovisku ÚOOÚ, kdy toto popisuje výjimečné situace, kdy zaměstnavatel může z důvodu ochrany svých práv otevřít e-mail zaměstnance. Mělo by být zřejmé, že email je pracovní a že z objektivních důvodů jej zaměstnanec nemůže zavčasu otevřít, a v tomto směru je potřeba zabránit případné hrozící újmě na zaměstnavatelových právech. Jako

[126] K tomu však srovnej výklad ESLP ve věci Bărbulescu v. Rumunsko níže.

[127] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 954

[128] Stanovisko ÚOOÚ č. 2/2009

[129] BÁRTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012*. 1. vydání. Olomouc: ANAG, 2012, s. 263

[130] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1244.

[131] Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele, s. 4, dostupné online na WWW <http://www.suip.cz/_files/suip-7eb7366515abb7d99bf593cba68221bc/ochrana_os.pdf>, [cit. 10.4.2018]

[132] MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, s. 6

příklad je uvedena dlouhodobá nemoc zaměstnance. Na druhou stranu dlouhodobá dovolená, kterou lze na rozdíl od nemoci předvídat, pro zaměstnavatele tímto důvodem není a tento má ještě před nástupem zaměstnance na dovolenou přijmout příslušná opatření k zastupování.[133]

O záměru monitorovat e-mailovou korespondenci musí zaměstnavatel své zaměstnance s ohledem na § 316 odst. 3) ZP (ale potažmo také § 11 ZOOÚ) pochopitelně informovat, podle názoru některých ideálně už při navazování pracovněprávního vztahu.[134]

Nyní ke konkrétním sporům ohledně sledování e-mailové komunikace, o kterých musel rozhodnout soud. Z poslední doby jedno z nejznámějších a mediálně nejrozebíranějších je bezesporu rozhodnutí ve věci Bărbulescu v. Rumunsko.[135] Ještě než přejdeme k rozboru samotného judikátu, autorka práce by ráda upozornila na fakt, že sedmičlenný senát ESLP v daném sporu nejprve poměrem hlasů 6 ku 1 rozhodl ve prospěch zaměstnavatele,[136] velký senát ESLP poté poměrem 11 ku 6 hlasům naopak zvrátil rozhodnutí ve prospěch zaměstnance, kdy shledal porušení ochrany stanovené čl. 8 EÚLP.[137] Demonstrativní, či chcete-li, výmluvný příklad, jak je v praxi posuzování střetu těchto dvou významných práv skutečně nelehká a komplexní otázka, kdy je třeba vzít v potaz konkrétní situaci, okolnosti, osoby atd. Takto se ostatně vyslovují i české soudy v případě rozhodování sporu v této oblasti. Viz např. rozhodnutí Nejvyššího soudu sp. zn. 21 Cdo 1771/2011: „*Ustanovení § 316 odst. 1 věta druhá zák. práce, patří k právním normám s relativně neurčitou hypotézou, které přenechávají soudu, aby podle svého uvážení v každém jednotlivém případě vymezil sám hypotézu právní normy ze širokého, předem neomezeného okruhu okolností*.“[138] Z těchto důvodů, je-li v této práci zmiňován

[133] Stanovisko ÚOOÚ č. 2/2009, či také PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 955

[134] BÁRTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012*. 1. vydání. Olomouc: ANAG, 2012, s. 263

[135] Rozhodnutí ESLP ve věci Bărbulescu v. Rumunsko, stížnost č. 61496/08

[136] Rozhodnutí ve věci ze dne 12. ledna 2016

[137] Rozhodnutí ve věci ze dne 5. září 2017

[138] Blíže k tomuto rozhodnutí v kapitole 4.3.3 Monitoring aktivity na PC

judikát, je vždy ve stručnosti uveden i krátký skutkový stav, neboť skutkové okolnosti hrají v případě posuzování legitimity monitoringu významnou a nezanedbatelnou roli.

Nyní zpět ke zmíněnému rozhodnutí ve věci Bărbulescu v. Rumunsko. Skutkový stav lze shrnout následovně: zaměstnanec na žádost zaměstnavatele zřídil firemní účet na Yahoo messengeru, který měl sloužit pro komunikaci se zákazníky. Na začátku července roku 2007 rozeslal zaměstnavatel svým zaměstnancům upozornění týkající se dodržování zákazu používání výpočetní techniky a telefonů pro soukromé účely a využívání pracovní doby pouze pro plnění pracovních úkolů. Tento zákaz byl taktéž zakotven ve vnitřních předpisech zaměstnavatele. S vnitřním předpisem i upozorněním byl dotčený zaměstnanec prokazatelně seznámen. Co se týče informace o možnosti monitoringu, tato byla zmíněna v uvedeném upozornění s tím, že dodržování pravidel pro používání výpočetní techniky bude sledováno a zjištěné prohřešky proti tomuto potrestány, jako exemplární příklad byla uvedena jistá zaměstnankyně, u které bylo porušování tohoto příkazu zjištěno, a proto s ní byl ukončen pracovní poměr.

V téže době, kdy bylo rozesíláno toto upozornění, zaměstnavatel prováděl několikadenní monitoring obsahu firemního Yahoo messengeru dotčeného zaměstnance. Díky tomuto zaměstnavatel zjistil, že zaměstnanec v pracovní době používá tento služební účet k soukromé konverzaci, mimo jiné se svým bratrem a snoubenkou (na některých místech obsahující intimní informace). Na žádost zaměstnavatele, aby se zaměstnanec vyjádřil k tomu, proč nedodržuje výše zmíněný zákaz, zaměstnanec odmítavě popřel jakékoliv porušování povinností, načež byl konfrontován s 45 stránkovým výpisem z firemního Yahoo messengeru, jehož obsahem byla zmíněná soukromá konverzace. Celá situace tak vyústila v podání výpovědi předmětnému zaměstnanci a tento naopak žaloval zaměstnavatele za nepřípustný zásah do soukromí.

Uvedený popis skutkového stavu je možná na první pohled relativně podrobný, ale skutečně je důležité shrnout sled událostí a zejména uvést situaci s ohledem na průběh informování zaměstnance o možnosti monitoringu.

Všechny vnitrostátní rumunské soudy zaměstnancovu žalobu zamítly a rozhodly ve prospěch zaměstnavatele, a to ve vztahu k výpovědi i ve vztahu k provedenému monitoringu. Stejný postoj pak zaujal i sedmičlenný senát ESLP ve svém prvním rozhodnutí. Podle něj nedošlo k porušení práva na soukromí, neboť zaměstnanec věděl o zákazu používání prostředků zaměstnavatele pro osobní účely a dále proto, že zaměstnavatel monitoroval pouze předmětný účet na Yahoo messengeru a dále argumentoval, že obsah tohoto byl zpřístupněn až poté, co zaměstnanec na výzvu k vysvětlení nedodržování zákazu reagoval negativně, že k ničemu takovému nedochází.

Jak již bylo zmíněno výše, velký senát ESLP vnímal celou situaci jinak. Podle jeho názoru zaměstnavatel předem dostatečně neinformoval o rozsahu a způsobu monitoringu a taktéž zaměstnance výslovně nevaroval, že může dojít i k přístupu k samotnému obsahu zpráv na účtu Yahoo messengeru. Dále velký senát kritizoval, že se žádný z jeho předchůdců nezaobíral otázkou, zdali nebylo možné zamýšleného účelu dosáhnout méně invazivními prostředky. V neposlední řadě podle soudu nebylo prokázáno najisto, kdy přesně zaměstnavatel sledoval obsah zpráv na předmětném účtu.

V tomto případě tedy zaměstnavatel prohrál spor zejména proto, že dostatečně nesplnil svou informační povinnost. Přitom o tom, že zaměstnanec, navzdory předcházejícímu apelu a upozornění, zneužíval pracovní dobu a zaměstnavatelem svěřené prostředky k nepracovním účelům, není pochyb.

Skupina WP29 k problematice soukromé konverzace v pracovní době uvádí, že vhodným řešením celé situace, kdy si zaměstnanci potřebují i v práci rychle vyřídit soukromou poštu, by bylo nabídnout zaměstnancům alternativní nemonitorovaný systém (buďto skrze síť WiFi s bezplatným připojením, nebo určené tablety s připojením na internet v prostorách pracoviště), na základě čehož by bylo umožněno zaměstnancům vykonávat své právo používat pracovní prostředky v rozumné míře pro soukromé účely.[139]

[139] Stanovisko Skupiny WP29 č. 2/2017, str. 14, dostupné online na WWW <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169>, [cit. 10.4.2018]

K tomuto je ovšem potřeba dodat, že české pracovní právo takové právo zaměstnance nezná. Ba naopak, jak je uvedeno výše, zaměstnanci mají zakázáno pracovní prostředky k těmto účelům bez svolení zaměstnavatele používat. Oporu pro tento názor pak lze nalézt i v literatuře, která uvádí, že nelze akceptovat, aby byli zaměstnavatelé nuceni do jisté míry tolerovat vyřizování soukromých záležitostí zaměstnance v pracovní době a skrze pracovní prostředky.[140] Jako zaměstnanecký benefit a opatření přispívající k zajištění ochrany soukromí zaměstnance na pracovišti by však takové řešení jistě nebylo nic proti ničemu.

4.3.2. Monitoring telefonů

Pro monitoring telefonů pochopitelně platí vše výše uvedené – tedy zaměstnavatel se musí při provádění kontroly opírat o legitimní důvody, zvážit přiměřenost zásahu do soukromí a o tomto ve stanoveném rozsahu informovat zaměstnance atd. Literatura se tomuto způsobu monitoringu nijak zvlášť zevrubně nevěnuje, zmiňováno je v této souvislosti především rozhodnutí Nejvyššího soudu sp. zn. 21 Cdo 1009/98.[141][142] Nejvyšší soud zde rozhodoval o okamžitém zrušení pracovního poměru, kdy bylo zaměstnanci vyčteno, že sabotuje společnost a přebírá její obchody na svou osobu. Jako důkaz společnost předložila přepis záznamů telefonických rozhovorů zaměstnance, které byly pořízeny bez jeho vědomí, přičemž se jednalo o hovory z pracovního telefonu. Soudu prvních dvou instancí tento důkaz odmítly provést z důvodu nepřípustného zásahu do soukromí zaměstnance, Nejvyšší soud pak tento jejich názor podpořil. Odposlouchávání telefonických hovorů je dle tohoto rozhodnutí zejména nepřípustné, nebyl-li zaměstnanec na možnost odposlechu upozorněn a důvodně tak očekával určitou míru soukromí. Nejvyšší soud se v argumentaci tohoto rozhodnutí opíral také o judikáty evropských soudů, zmíněn je např. ESLP Halford v. Velká Británie,[143] ve kterém je zmíněné vyjádřeno.

[140] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 945

[141] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1244.

[142] Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1009/98 ze dne 21. 10. 1998, publikován ve Sbírce soudních rozhodnutí a stanovisek pod č. R 39/99

[143] Rozhodnutí ESLP ve věci Halford v. Velká Británie ze dne 26. června 1997, stížnost č. 20605/92

Dalším relevantním judikátem je pak rozhodnutí Nejvyššího soudu sp. zn. 21 Cdo 747/2013.[144] V tomto případě zaměstnanec rozporoval výpověď z pracovního poměru, kterou od zaměstnavatele obdržel mimo jiné kvůli zneužití služebního telefonu pro soukromé účely a také služebního počítače, kdy měl v pracovní době na internetu vyhledávat soukromé záležitosti (a konečně také z důvodu pozdního příchodu do práce). Nejvyšší soud zaměstnancovu žalobu na neplatnost výpovědi zamítl, neboť uvedeným chováním se skutečně dopustil porušování svých povinností. Způsob provedení kontroly užívání svěřených prostředků blíže nezkoumal, seznal však, že důvodem kontroly nebylo zjistit obsah telefonických rozhovorů, ale pouze ověřit, zda zaměstnanec povinnost používat svěřené prostředky k pracovním účelům respektoval, což prokazatelně nedělal. Na straně zaměstnavatele v tomto směru tak nebylo zjištěno pochybení.

4.3.3. Monitoring aktivity na PC

Poslední zmiňovaný judikát nás přivádí k dalšímu způsobu kontroly zaměstnanců, a to ke sledování aktivity na služebním počítači. V tomto ohledu se promítne test proporcionality tak, že zaměstnavatel by měl nejprve pomocí technologických řešení zamezit vstup zaměstnancům na webové stránky a použití aplikací, které nepotřebují ke své práci. V tomto ohledu však literatura dále dodává, že na takovém řešení nelze bezpodmínečně trvat, mělo-li by pro zaměstnavatele představovat vynaložení nepřiměřených nákladů či úsilí.[145] Pokud se však o takovou situaci nejedná, pak lze tento způsob řešení označit za vhodný a právně bezvadný.[146]

Stanovisko ÚOOÚ č. 2/2009 připouští sledování webových stránek navštívených zaměstnanci při splnění všech zákonných podmínek, včetně závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele, pod kterou uvádí mezinárodní bankovní převody, či dozor nad prací vězňů. Pokud není splněna tato

[144] Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 747/2013 ze dne 7. 8. 2014

[145] MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, s. 404

[146] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 1244

podmínka, pak podle uvedeného stanoviska nelze monitorovat ani dobu strávenou prohlížením stránek nemajících vztah k vykonávané práci.[147]

Takový závěr je však pro praxi, zdá se, příliš striktní, neboť soudy připustily, aby tímto způsobem prováděl monitoring zaměstnavatel, jehož společnost se (zjednodušeně řečeno) zabývá montáží a výrobou dřevostaveb a truhlářských výrobků,[148] tedy nemusí se jednat o ÚOOÚ naznačovanou natolik specifickou povahu činnosti zaměstnavatele.

Přistoupí-li tedy zaměstnavatel kvůli důvodnému podezření na zneužívání pracovní doby a pracovních prostředků jeho zaměstnanců ke sledování jejich aktivity na PC, je oprávněn zpracovávat údaje v rozsahu datum, hodina, délka přístupu na webové stránky a míra aktivity zaměstnance na těchto stránkách.[149] Pokud má však zaměstnanec dovoleno (skrze vnitřní předpisy či pracovní smlouvu) užívat svěřené prostředky k osobním účelům, neměl by zaměstnavatel tyto informace v rámci této povolené doby zpracovávat.[150] K tomuto je ještě na místě poznamenat, že pokud zaměstnavatel takové použití svých prostředků povolí, musí podle názoru některých autorů vyjádřit svůj souhlas a k tomu přesně vymezit povolený rozsah takového užívání.[151]

K tomuto způsobu monitoringu se opět váží dva (resp. tři) významné judikáty. Prvním z nich je rozhodnutí Nejvyššího soudu sp. zn. 21 Cdo 1771/2011.[152] V daném sporu byl se zaměstnancem okamžitě zrušen pracovní poměr, neboť zaměstnavatel zjistil, že v průběhu jednoho měsíce zaměstnanec strávil na svém pracovním počítači bezmála 103 hodin nikoliv prací, ale s prací nijak nesouvisejícím prohlížením stránek na internetu. Zákaz takového používání počítače zaměstnavatel

[147] Stanovisko ÚOOÚ č. 2/2009 – Ochrana soukromí při zpracování osobních údajů, ve znění z února 2014, s. 4

[148] Viz rozhodnutí Nejvyššího soudu sp. zn. 21 Cdo 1771/2011 níže.

[149] MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, s. 405.

[150] Tamtéž, s. 405.

[151] BÁRTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012*. 1. vydání. Olomouc: ANAG, 2012, s. 258

[152] Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1771/2011 ze dne 16. 8. 2012

výslovně zakotvil v pracovním řádu pro zaměstnance. Důkazy o zaměstnancově aktivitě na počítači byly pořízeny bez jeho souhlasu a vědomí. Všechny soudy rozhodující v daném sporu rozhodly unisono – zaměstnavatel nijak nepřípustně nezasáhl do zaměstnancova soukromí, neboť nemonitoroval obsah korespondence, telefonů a ani jinak blíže nemonitoroval zaměstnancovu činnost na zakázaných stránkách, pouze v rámci výkonu práva na ochranu svého majetku ověřoval, zda tyto stránky byly navštíveny a v jakém časovém rozsahu. Důkaz získaný monitoringem zaměstnance je tak přípustný a taktéž odůvodňuje okamžité zrušení pracovního poměru, zvážíme-li zejména, že zaměstnanec v jednom měsíci strávil více než polovinu své pracovní doby nepracovní činností. Rozhodnutí soudů a jejich v tomto směru ústavně konformní intepretaci předmětných ustanovení ZP a ZOOÚ potvrdil Ústavní soud svým usnesením sp. zn. I. ÚS 3933/12.[153] K tomuto ještě poznámka, že v daném sporu tedy soudní praxe připustila možnost provedení skrytého monitoringu zaměstnanců, ač ohledně přípustnosti tohoto nepanuje v literatuře shoda (viz v úvodu kapitoly 4. výše).

Další zajímavý judikát pochází z pera španělského nejvyššího soudu, který dne 26. září 2009 rozhodl ve sporu propuštěného zaměstnance, bývalého generálního ředitele společnosti Corunesa de Etiquetas, S.L., pana Imanola.[154] V daném případě zaměstnanec v pracovní době navštěvoval nezabezpečené stránky, kvůli čemuž byl počítač napaden viry. Počítač proto odnesl z pracoviště technik a bez přítomnosti zaměstnance, či jeho zástupce jej prohlédl, načež zjistil, že v dočasně uložených souborech jsou data automaticky stažená při návštěvě stránek s pornografickým obsahem. Podruhé byla kontrola počítače provedena již za přítomnosti zaměstnance. Španělský nejvyšší soud v tomto případě shledal nepřípustný zásah do soukromí zaměstnance, kdy tento monitoring byl proveden bez jeho přítomnosti a vědomí, a zaměstnavatel se tak dostal k velice citlivým informacím. Soud také poukázal na to, že ačkoliv byl počítač umístěn v prostorách kanceláře tzv. open-space a pro přihlášení se do počítače nebylo vyžadováno žádné heslo, nejednalo se o určitý konkludentní souhlas zaměstnance, že by snad zaměstnavatel mohl bez jeho vědomí

[153] Usnesení Ústavního soudu I. ÚS 3933/12 ze dne 7. listopadu 2012

[154] Anglická anotace vyšla ve sborníku International Labour Law Reports 27, s. 109 – 123, jejíž kopii laskavě zapůjčil doc. Štefko.

do počítače kdykoliv nahlédnout. Kvůli tomuto pochybení, kdy bylo shledáno porušení čl. 8 EÚLP, nebyla výpověď daná zaměstnanci platná. Otázkou je, zda by české soudy rozhodly ve stejné situaci stejně, neboť španělský nejvyšší soud v odůvodnění taktéž zmínil, že zaměstnanec má právo využít zaměstnavatelovy prostředky v omezené míře k soukromým účelům. V českém právním řádu však toto bez souhlasu zaměstnavatele není možné (viz rozbor v kapitole 3.3.1. výše).

4.3.4. Kamery na pracovišti

Kamerové systémy na pracovišti (ale i obecně) lze rozlišovat na dva typy – systém se záznamem a bez záznamu. Rozdíl mezi těmito typy dříve ve svém důsledku představoval praktický a také reálný rozdíl ve způsobu, jaký orgán veřejné správy a za jakých okolností je oprávněn takový systému zaměstnavateli zakázat.[155]

Pokud má být využíván systém se záznamem, uplatní se jak úprava v ZP, tak v ZOOÚ, neboť bude při sledování zaměstnanců docházet ke zpracování osobních údajů ve smyslu ZOOÚ.[156] Systémy bez záznamu, které pak podléhají pouze režimu ZP, představují např. on-line tzv. webkamery.[157] Podle názoru autorky této práce se z důvodu novelizace znění ZIP tato dvojkolejnost již nadále zcela neuplatní. Oba typy kamerových systémů může totiž inspektorát práce, s odkazem na §§ 11a a 24a ZIP, sankcionovat, nejsou-li zavedeny v souladu se zákonem.

Stejně jako u jakéhokoliv jiného způsobu monitoringu, i zde je logicky zaměstnavatel vázán řadou povinnosti blíže rozebraných v kapitole 4.2. této práce.

Specifikum kamerového systému však je, že se jedná o jeden z nejzávažnějších zásahů do soukromí zaměstnance. K tomuto Nejvyšší správní soud ve svém rozhodnutí sp. zn. 5 As 1/2012 – 21: „*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*

[155] BÁRTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012*. 1. vydání. Olomouc: ANAG, 2012, s. 261

[156] NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7), s. 232

[157] Tamtéž, s. 233

schopny naplnit vytyčený účel, který je sledován."[158] V tomto směru se tedy silně projeví zásada proporcionality. Z tohoto důvodu je také třeba pečlivě zkoumat, zda jsou naplněny podmínky pro instalaci kamer na pracovišti. Podle literatury by se mělo zejména jednat o taková pracoviště, na nichž probíhá práce s velmi citlivými informacemi, utajovanými skutečnostmi nebo vyššími majetkovými hodnotami.[159]

Pokud se jedná o kamerové systémy bez záznamu, ve vztahu k těmto není potřeba plnit registrační povinnost vůči ÚOOÚ, neboť v rámci nich nedochází ke zpracování osobních údajů,[160] a proto na ně nedopadá § 16 ZOOÚ.

Ve vztahu ke kamerovým systémům se přidává pro zaměstnavatele ještě jedno omezení, a tím je maximální doba uchovávání záznamů. Pro soulad s právními předpisy by obecně neměly být uchovávány déle než 2 dny.[161]

Protože k tomuto nebyl vybrán žádný významný judikát, přejdeme dále k další formě monitoringu.

4.3.5. Kamera v kabině auta

Kamera v kabině služebního auta (či jiného vozu) zaměstnance je vlastně jedním z typů kamerového systému. Vyhrazena je mu však zvláštní podkapitola, a to z důvodu existence soudních rozhodnutí Nejvyššího správního soudu sp. zn. 10 As 245/2016 – 41,[162] který právě přípustnost kamery v kabině vozu řešil.

K povinnostem zaměstnavatele netřeba opakovat, co již bylo zmíněno v podkapitole 4.3.4. výše.

[158] Ze třetí právní věty rozsudku Nejvyššího správního soudu čj. 5 As 1/2011 - 156 ze dne 28. 6. 2013

[159] ZEMANOVÁ ŠIMONOVÁ, H.: Právní prostředky ochrany osobnosti zaměstnance. *Bulletin advokacie*. 2016, **23**(10), s. 40

[160] Stanovisko ÚOOÚ č. 1/2006 - Provozování kamerového systému z hlediska zákona o ochraně osobních údajů, s. 1

[161] Stanovisko ÚOOÚ č. 1/2015 - Provozování kamery v motorovém vozidle se záběrem mimo toto vozidlo, s. 2

[162] Rozsudek Nejvyššího správního soudu sp. zn. 10 As 245/2016 – 41 ze dne 20. 12. 2017

V předmětném sporu byla tedy kamera umístěna v přední části autobusu tak, že snímala řidiče a stewarda. Zaznamenávala pouze obraz, nikoliv zvuk. Správní orgány tento kamerový systém zamítly, Městský soud v Praze pod sp. zn. 5 A 107/2013 - 38[163], který následně přezkoumával napadené rozhodnutí, se zcela ztotožnil s jejich argumenty. Zaměstnavatel se snažil potřebnost instalace kamery odůvodnit účelem ochrany svého majetku (zabránit krádeži hotovosti a zboží), dále bezpečností cestujících a možného přezkumu jejich stížností (např. zaměstnavatel měl zkušenosti se stížnostmi cestujících na některé řidiče, kteří údajně při řízení v době jízdy používali mobilní telefon) a souvisejícího případného použití záznamu při zjišťování příčin dopravní nehody, a nakonec též účelem ochrany zdraví zaměstnanců (dodržování přestávek apod.). K těmto Městský soud shodně s předešlými správními orgány uvedl, že v autobuse není hotovost takové hodnoty, aby bylo zavedení kamerového systému odůvodněno. V tomto směru účelu poslouží stejně tak uzamykatelný prostor a poučení řidiče. Zdali řidiči konají svoji práci, jak mají (tedy že se při řízení věnují pouze tomuto a nepoužívají při tom mobilní telefon), lze zjistit skrze svědecké výpovědi cestujících, případně namátkovou kontrolou. Pro zjišťování příčin dopravní nehody je snímek z kabiny spíše nepoužitelný, k tomuto lépe poslouží kamery umístěné snímající prostor před autobusem. Naopak vědomí neustálého monitoringu může řidičům přivodit větší stres, který naopak může vést k dopravní nehodě.

Nejvyšší správní soud ve svém rozsudku (výše zmíněném sp. zn. 10 As 245/2016 – 41) následně přisvědčil velké většině argumentace obsažené v předešlých rozhodnutích. Při aplikace ústavního testu proporcionality dospěl k tomu, že zvolený prostředek sice naplnil kritérium vhodnosti, nikoliv však již kritérium přiměřenosti.

Jak již tedy bylo zmíněno v předešlé podkapitole, kamerový záznam je natolik invazivní způsob monitoringu, že by k němu měl zaměstnavatel přistoupit až pokud žádné jiné prostředky neumožňují naplnění vytyčených cílů, anebo by je umožňovaly, ale byly nasazené a všechny selhaly.

[163] Rozsudek Městského soudu v Praze, sp. zn. 5 A 107/2013 – 38 ze dne 18. 10. 2016

4.3.6. Kontrola docházky na pracoviště

Následující kapitola bude věnována kontrole docházky zaměstnanců na pracoviště. Evidence docházky, tedy evidence odpracované směny sama o sobě nijak problematická ve vztahu k zásahu do soukromí zaměstnance není, jedná se totiž s ohledem na znění § 96 ZP dokonce o zaměstnavatelovu povinnost. Problém ovšem nastává v momentě, kdy se zaměstnavatel rozhodne vyměnit běžné varianty docházkových systémů (jako např. kniha příchodů/odchodů, elektronické karty, čipy, či jiné elektronické systémy evidence docházky) a eviduje docházku s využitím biometrických údajů zaměstnanců.

Takové možnosti evidence již dnes nejsou technologicky nedostupné, a tak řada zaměstnanců musí při vstupu do budovy či prostor zaměstnavatele nejprve prokázat svoji totožnost, a to tak, že k příslušnému čtecímu zařízení přiloží dlaň, či jednotlivé prsty (pro sejmutí otisků prstů), či je možno naskenovat sítnici oka pro identifikaci jednotlivých zaměstnanců apod. Identifikace zaměstnance pak slouží jednak k povolení vstupu do prostor a jednak k zaznamenání příchodu konkrétního zaměstnance (logicky samozřejmě obdobné platí pro odchod zaměstnance z pracoviště). Je pochopitelné, že tento systém lze jen stěží obejít tak, jak snadno se lze nechat zapsat do docházkové knihy kolegou, zapsat jiný než skutečný čas příchodu/odchodu či vypůjčit si (čipovou) kartu od jiného pracovníka a zaměstnavatelům proto z těchto důvodů implementují takový systém docházky. Nicméně s ohledem na znění § 4 písm. b) ZOOÚ jsou biometrické údaje takové, které umožňují přímou identifikaci nebo autentizaci subjektů údajů citlivým údajem. Z tohoto důvodu je pak třeba dodržet stanovená pravidla při jejich zpracování. Pokud je zaměstnavatel zachová, pak je v současnosti možné zvolit i takový způsob evidence docházky.

I při zpracování citlivých osobních údajů je třeba samozřejmě splnit informační povinnost ve vztahu k subjektu osobních údajů – tedy informovat

zaměstnance o účelu zpracování biometrických údajů zaměstnavatelem spolu s určením období, po které budou tyto zpracovávány.[164]

Dále je třeba pro zpracování citlivých osobních údajů obdržet výslovný souhlas subjektů údajů, nebo je možné využít výjimky z povinnosti zisku souhlasu stanovené v dalších ustanoveních ZOOÚ. S ohledem na povahu osobních údajů, kdy tyto citlivé údaje je potřeba zákonem ještě více chránit, již není relevantní v obecném úvodu právních titulů zmiňovaný § 5 ZOOÚ, nýbrž § 9 ZOOÚ, který se právě věnuje možnostem citlivé osobní údaje zpracovávat. V rámci tohoto ustanovení pak pro zaměstnavatele pak přicházejí v úvahu zejména přípustné důvody zpracování v § 9 písm. d) a písm. h) ZOOÚ, k čemuž také došel ÚOOÚ ve svém stanovisku, nicméně dodává, že zpracování biometrických údajů zaměstnavatelem sice lze využívat, ale spíše jen ve výjimečných situacích.[165]

Vedle varianty zpracovávání biometrických údajů při každém příchodu (a odchodu) z pracoviště existuje další varianta (jednodušší z pohledu plnění povinností zaměstnavatele a mírnější ve vztahu k zásahu do soukromí subjektu), a to taková, která sice na první pohled zahrnuje biometrické údaje, přitom však v rámci této k jejich uchovávání ani ke zpracování nedochází. Dnešní technologie nabízí možnost nasnímání zaměstnancovy dlaně, sítnice, či jiného biometrického údaje, a tyto jsou následně matematickými operacemi (algoritmy, kódováním apod.) dále přiřazeny k číselnému kódu či je biometrický obraz jinak zredukován. Biometrické údaje jako takové již pak tedy nadále nejsou nijak uchovávány, nejsou ani posléze rekonstruovatelné a stávají se volně nečitelnými. Při kontaktu s docházkovým systémem je tak zaměstnanec identifikován pomocí přiřazeného čísla či redukovaného obrazu s výše uvedenými vlastnostmi, a proto se v tomto směru tedy nejedná o zpracování a uchovávání citlivých údajů, k čemuž v úvahách dochází

[164] Viz § 9 písm. a) ZOOÚ.

[165] Dříve stanovisko ÚOOÚ č. 3/2009 – Biometrická identifikace nebo autentizace zaměstnanců, s. 4, aktualizované skrze stanovisko ÚOOÚ č. 1/2017, s. 5

jednak odborná veřejnosti,[166] ale také ÚOOÚ.[167] Při zachování tohoto postupu a dodržení dalších zákonných povinností, které vyplývají správci osobních údajů ze ZOOÚ,[168] pak lze takový docházkový systém připustit. A nejen to – vzhledem k tomu, že se bude jednat o zpracování „běžných" osobních údajů (tedy nikoliv citlivých osobních údajů ve smyslu § 9 ZOOÚ) za účelem plnění práv a povinností zaměstnavatele, bude se ke zpracování vztahovat výjimka stanovená v § 18 odst. 1) písm. b) ZOOÚ, tedy zaměstnavatel nebude povinen písemně oznámit ÚOOÚ předem takové zpracování údajů, což potvrzuje samotný ÚOOÚ.[169] S ohledem na režim zpracování „běžných" osobních údajů pak bude možné zavést takový docházkový systém i bez souhlasu zaměstnanců (za splnění podmínek v § 5 odst. 2) ZOOÚ). S prvotním poskytnutím biometrického údaje však musí výslovně souhlasit zaměstnanci vždy.[170][171]

Alespoň taková byla praxe a postoj ÚOOÚ doposud. S výhledem účinnosti GDPR lze ovšem v tomto směru očekávat změny. V nejnovějším sdělení ve vztahu k citovanému stanovisku č. 1/2017 ÚOOÚ upozorňuje, že po nabytí účinnosti GDPR pravděpodobně dojde ke změně výkladu úpravy, neboť tato „*Přináší podstatnou změnu v právním pohledu na technologie zpracovávající biometrické údaje, mj. také v tom, že uchovávání biometrických údajů, včetně šablon (template) a jejich zpracování za účelem identifikace osob, považuje za zpracování zvláštní kategorie*[172]

---

[166] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců.* 1. vydání. Praha: C.H. Beck, 2013, s. 119

[167] Stanovisko ÚOOÚ č. 3/2009 – Biometrická identifikace nebo autentizace zaměstnanců, s. 2 i Stanovisko ÚOOÚ č. 1/2017, s. 4

[168] Viz např. již zmíněný § 5 ZOOÚ – stanovení účelu zpracování, prostředků aj. ze Stanoviska ÚOOÚ č. 1/2017, s. 5: „*Zaměstnavatel musí důsledně splnit nejen shora uvedené povinnosti podle § 5, 9 a 16, ale dále také informační povinnost podle § 11 a povinnosti při zabezpečení osobních údajů podle § 13 - 15 zákona o ochraně osobních údajů.*"

[169] Stanovisko ÚOOÚ č. 1/2017, s. 4

[170] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců.* 1. vydání. Praha: C.H. Beck, 2013, s. 119

[171] Ke stejnému závěru vede i apel ÚOOÚ v již zmíněném stanovisku č. 3/2009, kterým se obrací na zaměstnance, kteří nechtějí zaměstnavateli poskytnout biometrický údaj, aby s tímto nevyslovili souhlas a podali podnět k ÚOOÚ.

[172] Přičemž zvláštní kategorie osobních údajů je novou terminologií pro citlivé osobní údaje. Srovnej čl. 9 GDPR a § 4 písm. b) ZOOÚ.

osobních údajů.“[173] Z uvedeného vyplývá, že tyto systémy využívající hashování a jiné matematické operace, které byly doposud ÚOOÚ tolerovány v intencích zpracování běžných osobních údajů, budou posuzovány přísněji. Je tedy možné, že tato dnes již několik let zaběhlá praxe v současné době dozná po nabytí účinnosti GDPR nemalých změn, kdy zaměstnavatelé budou v budoucnu, na rozdíl proti dnešku, potřebovat pro docházkové systémy výslovný souhlas zaměstnanců. ÚOOÚ v tomto směru dále slibuje vydání nového stanoviska ke zpracování biometrických údajů.[174]

Samozřejmě je před zavedením takových systémů, jako ostatně před zavedením jakéhokoliv monitoringu pracovníků, logicky doporučováno vždy zvážit přiměřenost takového opatření.[175]

Stranou pozornosti by neměl zůstat výklad ve vztahu k biometrickým údajům sloužícím pouze za účelem autentizace osoby pro vstup na pracoviště bez toho, aby snímání biometrických údajů sloužilo taktéž jako evidence docházky. Možnost zavedení takového systému (z důvodu střežení bezpečnosti objektu) je výslovně dána pouze zařízením s jaderně energetickými reaktory, tedy např. jaderným elektrárnám, a to na základě vyhlášky č. 361/2016 Sb. (dříve obdobně ve vyhlášce č. 144/1997 Sb.), o fyzické ochraně jaderných materiálů a jaderných zařízení. U ostatních zaměstnavatelů by tak zavedení tohoto systému při pouhém sledování účelu bezpečnosti objektu zřejmě neobstálo.[176]

---

[173] Sdělení ÚOOÚ vydané dne 13. března 2018, dostupné on-line na WWW: <https://www.uoou.cz/upozorneni-na-zmenu-v-nbsp-posuzovani-systemu-vyuzivajicich-biometricke-udaje-drive-quot-stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu-quot/d-29048/p1=2247>, [cit. 10.4.2018]

[174] Ke dni uzavření rukopisu 2. 5. 2018 nebylo stanovisko zveřejněno.

[175] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců.* 1. vydání. Praha: C.H. Beck, 2013, s. 120

[176] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců.* 1. vydání. Praha: C.H. Beck, 2013, s. 120 - 121

4.3.7. Monitoring pomocí GPS

Poslední konkrétní možností, jak sledovat zaměstnance, které bude věnována pozornost, je monitoring za využití GPS přístrojů. Tato zařízení umožňují určit velice přesně polohu objektu a i tato jsou dnes lehce dostupnou technologií. GPS může být zabudována do služebního automobilu, nebo může být takovým zařízením umožňujícím určení lokace vybaven přímo zaměstnanec.

Zásady spojené s monitorováním za pomocí kamerových systémů lze aplikovat i na tento druh monitoringu.[177] Takové sledování může sloužit k řadě účelů, diskutován bude dále účel ochrany majetku.

V případě instalace takového aparátu do zaměstnavatelova automobilu lze pak rozlišovat dvojí typovou ochranu majetku zaměstnavatele. První variantou může být ochrana samotného vozu. Dojde-li totiž ke krádeži, usnadňuje GPS zařízení lokaci odcizeného vozidla. V případě zaměstnavatele např. bankovní instituce, jehož zaměstnanci ve vozidlech rozvážejí a doplňují bankovky do jednotlivých poboček či bankomatů, lze jistě identifikovat sílu a legitimitu takového argumentu, a to tím spíše, má-li zaměstnavatel s útoky na majetek, tedy na svá vozidla či přepravované peníze, již historicky negativní zkušenosti.[178]

Druhou variantou (ve vztahu k ochraně majetku zaměstnavatele, jak již bylo výše zmíněno) je kontrola plnění pracovních povinností zaměstnance. Pomocí GPS zařízení lze totiž kontrolovat ujetou trasu vozidla, tedy zda zaměstnanec využívá auto skutečně ke služebním účelům, případně má-li zaměstnanec povoleno užívat automobil i k soukromým účelům, zda dodržuje rozsah tohoto oprávnění (byl-li sjednán), či zda zaměstnanec v pracovní době skutečně podnikl služební cestu, nebo nikoliv. Ochrana majetku zaměstnavatele před krádeží či úmyslným zneužíváním však nemusí být jediný účel zavedení GPS monitoringu.

---

[177] Stanovisko Skupiny WP29 č. 4/2004, s. 2, dostupné online na WWW <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22427> [cit. 30.3.2018]

[178] Viz obdobně KADLECOVÁ, T. GPS ve služebních vozidlech aneb malý čip = velká komplikace? *Praktická personalistika*, 2015, **1**(3-4), s. 10

Legitimní je podle názoru některých taktéž zavedení GPS zařízení za účelem zefektivnění činností, zrychlení a zkvalitnění poskytovaných služeb pomocí optimalizace tras.[179] Zaměstnavatel tedy v takovém případě nechce zaměstnance kontrolovat, pouze se snaží pomocí sběru dat optimalizovat poskytování svých služeb. Je otázkou, zda by v případném sporu podle soudu takové řešení splnilo test proporcionality, zvláště pokud by před nasazením GPS zařízení zaměstnavatel nevyzkoušel jiné možnosti, jak zefektivnit své služby (viz rozsudek Nejvyššího správního soudu v podkapitole 4.3.5. o kameře v kabině vozu).

Mnohem legitimnější okolnosti pro zavedení monitoringu pomocí GPS představuje situace, kdy má zaměstnanec výslovně zakázáno používat služební automobil k jiným účelům než k výkonu práce, a zaměstnavatel má důvodné podezření, že zaměstnanec opakovaně tento zákaz porušuje, a navíc pokud by zároveň byl zaměstnanec explicitně zaměstnavatelem upozorněn, že na základě těchto podezření může dojít ke kontrole korektního využívání služebního automobilu. Ve vztahu k takové situace se lze dočíst, že tato nepodléhá registrační povinnosti vůči ÚOOÚ dle § 16 ZOOÚ, neboť se uplatní výjimka podle § 18 ZOOÚ.[180]

Dokonce pokud by zaměstnavatel skrze GPS technologie provedl pouze jednorázovou a namátkovou kontrolu, zda zaměstnanec plní své pracovní povinnosti, či pokud by došlo k využívání GPS zařízení jen po omezenou dobu pro účely zefektivnění služeb, pak se podle některých vůbec nejedná o monitoring zaměstnance, a tím pádem by se úprava v ZP neměla vůbec aplikovat.[181]

Logický je závěr, že pokud může zaměstnanec služební automobil využívat i pro soukromé účely, bylo by v rozporu s právními předpisy monitorovat polohu

[179] RADIČOVÁ, Z. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy.* 2014 **22(**21), s. 736

[180] Tamtéž, s. 736

[181] RADIČOVÁ, Z. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy.* 2014 **22(**21), s. 737

vozu mimo pracovní dny a pracovní dobu.[182] Zaměstnavatel tedy musí v tomto směru zabezpečit, aby k takovému sběru dat nemohlo dojít.

I k tomuto typu monitoringu lze zmínit jedno významné soudní rozhodnutí. V daném případě se tedy nejednalo o spornou instalaci GPS do vozu, ale o vybavení takovým lokalizátorem zaměstnance. Řeč je o rozsudku Městského soudu v Praze sp. zn. 6 A 42/2013 – 48.[183] V předmětném sporu vybavila společnost Česká pošta, s.p. všechny své zaměstnance na pozici listovního doručovatele GPS trackerem, který zaznamenával kompletní informace o pohybu daného doručovatele, tedy včetně např. délky trasy, času stráveného na trase, obslužnosti okrsku, všechna navštívená i nenavštívená doručovací místa atd. Informace byly shromažďovány systematicky po dobu bezmála jednoho roku, bez souhlasu zaměstnanců. Na základě provedené kontroly uložil ÚOOÚ danému zaměstnavateli pokutu, neboť dle jeho názoru je takové zpracovávání osobních údajů v rozporu se zákonem. Zaměstnavatel se bránil soudní cestou, Městský soud dal však za pravdu ÚOOÚ.

Zaměstnavatel udával jako účel tohoto opatření optimalizaci doručování, nikoliv sledování konkrétních zaměstnanců. V tomto směru se také bránil tím, že data byla zaznamenávána bez odkazu na konkrétního zaměstnance, kdy ztotožnění s tímto konkrétním zaměstnancem sice nebylo technicky nemožné, ale dle jeho slov velice náročné. Tuto potvrzenou náročnost ÚOOÚ rozporoval, podle rozpisu směn lze zjistit, který doručovatel obsluhoval ten den daný okrsek. Soud potom při posouzení dále také došel k tomu, že uvedeného účelu (optimalizace doručování) šlo dosáhnout i jinými, méně invazivními způsoby, které zaměstnavatel ani neuvážil. Dále shodně s ÚOOÚ vytýkal široký rozsah doby a způsob zpracování. Kontrola mohla proběhnout namátkově, či po několik dní, nikoliv nepřetržitě po dobu celé směny v průběhu téměř jednoho celého roku. Konečně zvolený prostředek nebyl ani vhodným, neboť v rámci obrany zaměstnavatel uváděl, že má s ohledem na svou činnost odpovědnost za zabezpečení a řádné doručování svěřených zásilek, nepřetržité monitorování trasy však nemohlo zabránit případnému

[182] Tamtéž, s. 739

[183] Rozsudek Městského soudu v Praze sp. zn. 6 A 42/2013 – 48 ze dne 5. 5. 2017

nedoručení pošty. Informace, že se doručovatel na místě vyskytl, neznamená, že zásilka byla řádně předána.

S ohledem na dosud popsané povinnosti a omezení, kterých musí zaměstnavatel při monitoringu dbát, pak takové rozhodnutí není nijak překvapivé.

4.4. Další formy kontroly – monitoring zaměstnance klientem zaměstnavatele

Zajímavou otázku ve vztahu k předmětu diplomové práce rozvádí Kolegium AKV v jednom ze svých stanovisek.[184] Chráněným objektem je stále soukromí zaměstnance, nicméně zasahujícím do něj nemá být tentokráte zaměstnavatel, ale pacient či klient, kterému zaměstnanec poskytuje služby v rámci svého povolání. Nejen zaměstnavatelé dnes totiž snadno dosáhnou na různé technologické prostředky – ve stanovisku je zmiňována kamera v mobilním telefonu, za pomocí níž má dojít k pořízení videozáznamu zaměstnance konajícího práci (lékaře, učitele atd.). Kolegiu byl položen dotaz, zda se dá považovat za porušení pracovní kázně, pokud zaměstnanec odmítne výkon práce, a to právě s odůvodněním, že si nepřeje, aby došlo k takovému zásahu do jeho soukromí.

Kolegium přistoupilo k řešení otázky za pomocí užití známého testu proporcionality, který byl přiblížen výše v kapitole 4. a v průběhu práce několikrát zmíněn. Tedy že je potřeba zohlednit, zdali je pořízení videozáznamu jediným možným prostředkem pro ochranu práv dotyčné nahrávající osoby. Podle Kolegia neexistuje jednoduchá všeobecná odpověď, nýbrž je nutné vždy posoudit konkrétní situaci a okolnosti vedoucí osobu k pořízení záznamu.[185]

Například je uveden jako jeden z aspektů samotné povolání zaměstnance, tedy že jinak vystupuje zaměstnanec veřejné sféry (úřední osoba, která plní své úkoly ve veřejném zájmu) a jinak zaměstnanec soukromého zaměstnavatele. Kolegium nicméně dospělo k názoru, že se jedná o natolik závažný zásah

[184] Výkladová stanoviska AKV (XIX.), přijatá na zasedání Kolegia expertů AKV v Kolíně ve dnech 4. a 5. 11. 2016 – IV. část, část 27.

[185] I toto již bylo v souvislosti s monitoringem nejednou zmíněno.

do ochrany podoby a soukromí zaměstnance, že ve většině případů zaměstnancova práva převáží, a v tom případě pak nebude moci zaměstnavatel posuzovat odmítnutí výkonu práce jako porušení pracovní kázně. I pro tyto situace je pak doporučeno zaměstnavatelům, aby vymezili, za jakých podmínek bude možné po zaměstnanci požadovat výkon práce i přes probíhající monitoring.

5. Porovnání s úpravou Velké Británie

5.1. Úvod

Jak již bylo předestřeno v úvodu práce, následující kapitola přináší krátký exkurz do problematiky v rámci zahraniční jurisdikce, a to konkrétně do oblasti tzv. Common Law systému – blíže pak právního rámce Velké Británie – jurisdikce Anglie a Walesu (dále jako „*Anglie*“ či „*anglická*“ právní úprava). Právní úprava Common Law a systému kontinentální Evropy je, jak známo mnohdy postavená na naprosto protichůdných principech. Kde v tuzemském řádu rozvádí norma ochranu zaměstnance, může v Anglii srovnatelná zakotvovat ochranu zaměstnavatele a naopak.[186]

Český ZP, resp. soudy a odborná veřejnost se při jeho výkladu práce nadto netají tím, že jako celkem jím prostupuje zásada ochrany zaměstnance, nežli by nastavoval

[186] Právní úprava Anglie například nezná zákonnou povinnost k náhradě škody způsobené zaměstnavateli, tak jak ji najdeme v § 250 an. ZP. Strany si toto musí smluvně upravit. Viz např. soudce Lord Denning v soudním rozhodnutí Eric Morris v. Ford Motor Company [1973] EWCA Civ J0327-1: „*The servant would feel extremely aggrieved if sued by the employer or its insurance company – the worker would comment that the master takes the benefit of his labour and should bear the burden, and that the wages are fixed on that basis.*“ Ačkoliv se jedná o rozsudek staršího data, stále je aktuální a citovaný – viz např. online článek z 26. 6. 2015, dostupný online na WWW <https://hdm.ie/can-employers-sue-employees-for-insured-wrongs/ >, [cit. 11.4.2018]; A naopak, v porovnání s českou právní úpravou v ZP, je zaměstnancova ochrana v Anglii oslabena například při ukončování pracovního poměru, např. výpovědní doba může činit i pouze 1 týden, viz část 86 (1) Employment Rights Act 1996.

rovné postavení obou stran a ani jedné z nich nenadržoval[187] (jak je tomu například v zásadě v občanském právu, které až na výjimky přiznává stranám rovné postavení).

Co se porovnání týče, je ovšem v oblasti ochrany osobních údajů velmi znát vliv evropské harmonizace, tedy při srovnání obou úprav vlastně nelze nalézt větších rozdílů. Otázkou je, co s tímto závěrem učiní tzv. Brexit, tedy odchod Velké Británie z EU. Pokud tedy v tomto směru nedojde k žádné změně, ode dne 30. března 2019 totiž přestanou pro Velkou Británii platit veškeré normy primárního a sekundárního práva EU. V této souvislosti s ohledem na zpracování osobních údajů proto Evropská komise s předstihem zveřejnila informační sdělení, jaký by měl být další postup a co Brexit na poli ochrany osobních údajů znamená.[188]

5.2. Soukromí „anglického“ zaměstnance

Zpět k současné, účinné právní úpravě. Co se týče oblasti ochrany soukromí zaměstnance v anglické jurisdikci, je třeba v prvé řadě zmínit judikatorně dovozenou závaznost právní zásady zvané „*duty of mutual trust and confidence*“ v pracovněprávním vztahu,[189] tedy volně v překladu zásady vzájemné důvěry a důvěrnosti. Tato právní zásada sice není nikde v zákoně zakotvena, nicméně výkladem práva soudci došli k její existenci a platnosti a uplatní se tak v rámci každého pracovněprávního vztahu nehledě na konkrétní smluvní ujednání.[190]

Neoprávněný zásah do zaměstnancova soukromí, tedy zásah bez řádného důvodu či bez aprobace právní normou („*without pursuance to the law*“), může být posouzen jako porušení této dovozené zásady. Dokonce i v případě pokusu o neoprávněný zásah

[187] BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář*. 2. vydání. Praha: C. H. Beck, 2015, s. 5 či s. 1220, v judikatuře pak např. rozhodnutí Nejvyššího soudu sp. zn. 21 Cdo 4659/2016 ze dne 1. 6. 2017 atd.

[188] Blíže viz ve sdělení Evropské komise ze dne 9. ledna 2018, dostupné online na WWW <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=611943>, [cit. 2.4.2018]

[189] Rozhodnutí ve věci Malik v Bank of Credit and Commerce International SA (In Liquidation) [1997] I.C.R. 606

[190] V odborných textech je tento typ zásady označován jako dovozený, tedy jako „implied.“ Jedná se o takové zásady, které nelze nalézt nikde výslovně v právním řádu zakotvené, ani se nejedná o zásady sjednané smluvními stranami, nicméně byly soudci dovozeny jako existující a platné, vyplývající z legislativy. Zásady českého pracovního práva můžeme nalézt výslovně zakotvené např. v § 1a ZP.

můžeme hovořit o stejném výsledku, tedy o porušení tohoto principu, a to například v situaci, kdy zaměstnavatel nikoliv v souladu se zákonem požádá o sdělení nějaké osobní informace či osobního údaje "*Once the employment has begun, an employer´s request for private information could amount to a breach of the duty of mutual trust and confidence.*"[191]

Následkem porušení této zásady pak může být úspěšná žaloba na náhradu škody, nebo úspěch při žalobě na určení zvláštního typu skončení pracovního poměru tzv. „*constructive dismissal".*[192] Anebo až v extrémních případech může být neoprávněný zásah zaměstnavatele do zaměstnancova soukromí, tzv. „*unlawful interception*"[193] potrestán pokutou či dokonce trestem odnětí svobody, nebo kombinací obojího.[194][195]

Z důvodu (stále ještě aktuální) evropské integrace Velké Británie je stěžejním i v anglickém právním řádu Článek 8 EÚLP, který přiznává každému práva na soukromí a rodinný život, jehož obsah byl taktéž inkorporován do Článku 8 Přílohy 1 Zákona o lidských právech („*the Human Rights Act*").[196]

V této 5. kapitole je problematika zkoumána v rámci dvou subkategorií – (i) osobní údaje zaměstnance a (ii) soukromí zaměstnance na pracovišti. Ani v anglickém právním řádu není právo na ochranu soukromí zaměstnance absolutní a jisté zásahy zaměstnavatele mohou být legitimní. Stejně jako v České republice, tak i v Anglii lze identifikovat právo zaměstnavatele na ochranu svého majetku.[197]

---

[191] DEAKIN, S., MORRIS, G. *Labour Law.* 6. vydání. Portland, Oregon: Hart Publishing, 2012, s. 386

[192] O *constructive dismissal* hovoříme v situaci, kdy zaměstnanec podá výpověď, ale jako výpovědní důvod udá zaměstnavatelovo nepřijatelné chování - porušování jeho povinností, nebo zaměstnancových práv. Úspěch ve věci opět vede k odškodnění; constructive dismisal je pak upraven v zákoně The Employments Right Act 1996 část 95 (1) (c)

[193] Viz Regulation of Investigatory Powers Act 2000 článek 1 (1)

[194] Viz Regulation of Investigatory Powers Act 2000 článek 1 (7)

[195] Podle názoru autorky se jedná o jednu z oblastí právních úprav, kde je srovnání z důvodu rozdílnosti zajímavé – v České republice takové chování zaměstnavatele spíše není možné sankcionovat tak závažným trestem, viz rozbor v části 2.2.4.

[196] Human Rights Act 1998, znění ze dne 8. 4. 2018

[197] V originálním znění „*right to protect employer's legitimate business interests*".

5.2.1. Ochrana osobních údajů

Shodně s Českou republikou, i ve Velké Británii lze nalézt zákon samostatně upravující ochranu osobních údajů – „*Data Protection Act*“ (dále jako „*DPA*“).[198]

Naproti tomu ve Velké Británii neexistuje přímo ekvivalent českého ÚOOÚ, úřadu specializujícího se pouze na ochranu osobních údajů. Stížnosti týkající se nakládání s osobními údaji, avšak spolu s dalšími stížnostmi v oblastech, jakými jsou např. ochrana práva na informace a práva na informace o životním prostředí, má ve své kompetenci úřad zvaný *Information Commisioner's Office* (dále jako „*ICO*“). Stejně jako ÚOOÚ napomáhá správcům osobních údajů (včetně zaměstnavatelů pochopitelně) s výkladem zákonných povinností skrze vydávání stanovisek apod., tak i zmíněný ICO v tomto směru vyvíjí aktivitu, zejména významným je skoro stostránkový *Employment Practices Code*[199] (dále jako „*EPC*“), který je celý věnován právě zpracování osobních údajů zaměstnavatelem.

Definice osobních údajů a stejně tak citlivých osobních údajů, osoby správce a zpracovatele jsou v zásadě obsahově totožné s definováním těchto českým právním řádem.[200] Nejedná se o podobnost náhodnou, oba dva předpisy – jak ZOOÚ, tak DPA implementují Směrnici.[201]

---

[198] Data Protection Act 1998, znění ze dne 8. 4. 2018

[199] The Informational Commissioner's Office, *The Employment Practices Code on Data Protection* dostupný online na WWW <https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf>, znění z 8. 4. 2018

[200] Podle DPA čl. 1 odst. (1): "*Personal data means data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller*". Srovnej s § 4 písm. (a) ZOOÚ. Správce osobních údajů je pak definován tamtéž (čl. 1 odst. (1) DPA): "*The data controller is a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed"*. Srovnej s § 4 písm. (j) ZOOÚ. A dále např. definice zpracovatele, v témže ustanovení DPA: "*Any person (other than an employee of the data controller) who processes the data on behalf of the data controller."* Srovnej s § 4 písm. (k) ZOOÚ, obsahově podobná je také definice citlivých osobních údajů v čl. 2 DPA a § 4 písm. (b) ZOOÚ atd.

[201] K českému zákonu viz důvodová zpráva k návrhu ZOOÚ, sněm. tisk 374/0, ze 3. období Poslanecké sněmovny (1998 – 2002), s. 1; k DPA pak publikace "*An overview of UK data protection law*", s. 1, dostupná online na WWW <https://united-kingdom.taylorwessing.com/uploads/tx_siruplawyermanagement/NB_000168_Overview_UK_data_protection_law_WEB.pdf>, [cit. 11.4.2018]

Z výše uvedeného plyne, že i v Anglii je nastavení stejné a při zpracování osobních údajů nastavena potřeba v zásadě získat souhlas subjektů. DPA formu souhlasu nijak nespecifikuje (vyjma výslovného souhlasu při zpracování citlivých osobních údajů).[202] Nicméně v příloze č. 2 k DPA stojí, že titulem pro zpracování údajů může být účel ochrany legitimních zájmů zpracovatele.[203]

S ohledem na to je dovozováno, že pokud zaměstnavatel prokáže, že jsou osobní údaje jeho zaměstnanců zpracovávané za účelem zajištění ochrany jeho oprávněných zájmů, a do soukromí není zasahováno nad rámec zaměstnancova legitimního očekávání, výslovný souhlas není potřeba získat.[204] Potud k základu, který je v obou úpravách, dá se říct, shodný. Nyní se zaměříme spíše na ta místa, kde lze nalézt rozdíly, než abychom se věnovali legislativně harmonizovaným oblastem.

Stejně jako v české právní úpravě podle § 12 ZOOÚ, má i podle anglické právní úpravy subjekt právo na přístup k informacím.[205] V ČR není zneužívání tohoto práva rozšířeným jevem,[206] v Anglii je ovšem situace zřejmě jiná, a proto může být toto právo zpochybňováno, jak vyplývá např. ze soudního rozhodnutí ve věci Elliott v. Lloyds TSB Bank: "*The dominant purpose for the subject access request was a fishing expedition to further his claims against Lloyds*". [207] Z tohoto důvodu soud rozhodl o tom, že takové zneužití práva nepožívá právní ochrany a subjekt údajů tak nemá právo na přístup k požadované informaci o zpracování svých osobních údajů. I z dalších zdrojů vyplývá, že tento přístup skutečně není ojedinělý a že obdobná situace vyskytla i v dalších sporech.[208]

---

[202] DPA Příloha (Schedule) 3 část 1, znění ze dne 8. 4. 2018

[203] DPA Příloha (Schedule) 2 část 6 (1), znění ze dne 8. 4. 2018

[204] BOND, R., PROTOKOVA, V. Monitoring in the workplace - damned if you do and damned if you don't! *Compliance & Risk,* 2015, 4(3), s. 2-5: "*If an employer can validly show that processing is required to ensure the pursuit of its legitimate interest, the candidate's consent is not required provided that the processing does not interfere with the privacy expectations of the individual.*"

[205] DPA Čl. 7

[206] NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související: komentář*. 1. vydání. Praha: Wolters Kluwer ČR, 2014, s. 217.

[207] Elliott v Lloyds TSB Bank Plc & Anor [2012] EW Misc 7

[208] Autor neuveden. Subject access request by employees – 2. *IDS Emp. L. Brief* 2015, 1025, s. 15

5.2.2. Monitoring zaměstnanců

Jistá dvojkolejnost, se kterou je potřeba pracovat v českém právním řádu pro hodnocení legálnosti monitoringu zaměstnanců, v anglickém neexistuje. Možnost provádět sledování zaměstnanců se odvíjí pouze od zákona o ochraně osobních údajů – DPA: „*The Data Protection Act does not prevent an employer from monitoring workers, but such monitoring must be done in a way which is consistent with the Act. Employers – especially in the public sector – must also bear in mind Article 8 of the European Convention on Human Rights."*[209]

Jak patrno z vybraného úryvku, v Anglii se při hodnocení monitoringu dále zohledňuje, zda jde o zaměstnavatele ze soukromého, či státního sektoru. To je naopak určitá dvojkolejnost, kterou u soudního hodnocení monitoringu v české úpravě nijak vyzdviženou nenajdeme.

Článek 8. odst. 2) EÚLP totiž obsahuje výjimky ze zákazu zasahování do soukromí osoby, které se vztahují na státní orgány. Tyto výjimky pak ve sporu McGowan v. Scottish Water[210] ospravedlnily nasazení soukromého detektiva na zaměstnance. Detektiv čekal schovaný poblíž zaměstnancova domu, aby jej natočil ve chvílích, kdy opouštěl domov a kdy se do něj vracel. Účelem tohoto záznamu pak bylo prokázat, zda zaměstnanec vykazuje svoji pracovní dobu pravdivě. Vzhledem k tomu, že zaměstnavatel spravoval vodovodní potrubí, odvolací soud uznal, že takový zásah do soukromí zaměstnance byl odůvodnitelný veřejným zájmem, kdy při nedostatečné péči a plnění pracovních povinností zaměstnance hrozila porucha potrubí a následné havárie. Veřejný zájem tedy převážil individuální zájmy jedince. Stěží si lze představit stejné rozhodnutí podle českého práva. Podle názoru autorky lze pravdivost pracovního výkazu ověřit i méně invazivními metodami, nasazení detektiva v utajení by tak zřejmě nesplnilo podmínky testu proporcionality.

[209] EPC, s. 58, znění ze dne 8. 4. 2018

[210] McGowan v Scottish Water [2005] IRLR 167

Dalším právním předpisem, který na monitoring zaměstnanců dopadá a který taktéž bere v potaz EPC, je „*Regulation of Investigatory Powers Act"* (dále jako „*RIPA*").[211] Účelem tohoto předpisu je stanovit hranici mezi soukromím jedince a potřebou korporací vytěžit maximum z investic do telekomunikačních technologií.[212] Tento právní předpis v zásadě obecně definuje, za jakých podmínek je odposlech legitimní a dopadá tak i na sledování, resp. odposlech zaměstnanců.

EPC zaměstnavatelům s odkazem na DPA a zmíněný RIPA doporučuje, stejně jako odborná literatura vykládající českou právní úpravu, před zavedením monitoringu nejprve provést posouzení dopadů zamýšleného záměru sledovat zaměstnance.[213]

Stejně jako v české právní úpravě, i v anglické je povinností (až na možné výjimky) informovat zaměstnance o monitoringu, toto zdůrazňuje jak EPC: "*Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified,*"[214] tak relevantní odborná literatura.[215]

Co už ovšem EPC nezmiňuje, je registrační povinnost příslušnému úřadu – ICO, byť jen v určitých případech provádění monitoringu. Článek 18 DPA sice obecnou registrační povinnost zpracovatelů obsahuje, nicméně tato není ve vztahu k monitoringu v EPC zdůrazněna. Zmíněna je až v dalším kodexu – příručce vydaným taktéž ICO, a to v kodexu s názvem „*Data Protection Code of Practice for Surveillance Cameras and Personal Information*", zkráceně taktéž označovaném

[211] Regulation of Investigatory Powers Act 2000, znění ze dne 8. 4. 2018

[212] BOND, R., PROTOKOVA, V. Monitoring in the workplace - damned if you do and damned if you don't! *Compliance & Risk,* 2015, **4**(3), s. 2-5

[213] Obsahem posouzení je tak logicky identifikovat účel pro monitoring, zda je tento schopen dosáhnout požadovaného cíle, dopady monitoring na soukromí zaměstnance, a především zvážení vhodných alternativ pro dosažení cíle. Viz EPC, s. 61, ve znění ze dne 8. 4. 2018

[214] EPC, s. 65, ve znění ze dne 8. 4. 2018

[215] SAKROUGE, A., a kol. Monitoring employee communications: data protection and privacy issues. *C.T.L.R.* 2011, **17**(8), s. 213-216

„*CCTV Code of Practice*", který přináší návod, jak postupovat v případě zavádění a využívání kamerových systémů.[216]

Dále je vhodné zmínit, že EPC výslovně povoluje skrytý monitoring, neboť i k této formě sledování přináší výklad, jak v uvedeném případě postupovat.[217] V porovnání s českým právním prostředím – ohledně této formy monitoringu zde nepanuje shoda, viz příslušná kapitola 4. výše. Celkem se pak přímo tématu sledování zaměstnanců věnuje 20 stránek EPC, kde zaměstnavatelé najdou poměrně podrobný návod a konkrétní příklady, jak postupovat.

5.3. Závěr k porovnání s úpravou Velké Británie

S ohledem na výše uvedené lze uzavřít, že mezi právní úpravou ČR a Anglie (zatím) nelze nalézt větších rozdílů, neboť v tomto směru se do obou právních řádů významně prosadila evropská harmonizace. Otázkou je, jak se situace promění po odchodu Velké Británie z EU.

K těm zajímavějším rozdílům lze zmínit možnou trestní odpovědnost zaměstnavatele při postupu v rozporu se zákonem, dále v Anglii musí brát zaměstnavatele v potaz jen úpravu v DPA – v zákoně o ochraně osobních údajů, který jediný jim monitoring povoluje (neboť jim ho výslovně nezakazuje), žádnou obdobu podobné úpravy v obdobném pracovněprávním kodexu či předpisu jakým je v České republice ZP v Anglii nenalezneme. Za potenciálně rozdílné by se dalo označit posuzování nasazení soukromých detektivů na zaměstnance za účelem kontroly pracovní doby, obdobné rozhodnutí v české první úpravě však není dostupné. Konečně lze jako odlišné zmínit podrobnější návod oficiálně vydaný úřadem zabývajícím se, mimo jiné, ochranou osobních údajů.

[216] Např. viz CCTV Code of Practice s. 12, dostupného online na WWW <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>, znění ze dne 8.4.2018

[217] EPC, s. 74, znění ze dne 8. 4. 2018

6. Závěr

Tématem této diplomové práce byla problematika monitoringu zaměstnanců. Sledování zaměstnanců potenciálně ohrožuje zaměstnancovo právo na soukromí, zároveň pak ke sledování dochází z důvodu potřeby ochrany dalšího významného práva – práva na ochranu zaměstnavatelova majetku, jeho vlastnictví. V tomto ohledu lze jinými slovy s nadsázkou říct, že zvoleným tématem práce byla kolize dvou základních lidských práv.

Cílem práce bylo jednak přiblížit relevantní právní úpravu, dále pak diskutovat konkrétní, či alespoň přibližné hranice možnosti výkonu legálního monitoringu. S ohledem na faktory, které v tomto směru hrají důležitou roli, byla věnována pozornost také vybraným soudním rozhodnutím, neb tato nejlépe demonstrují, jak komplexně je třeba monitoring posuzovat a kde se tato hranice nachází.

Nejprve se práce zaobírala obecnou právní úpravou práva na ochranu soukromí a ochranu osobních údajů člověka. Neboť právě tato jsou monitoringem potenciálně zasažena a také, jak již bylo zmíněno výše, zaměstnanec je zejména osoba a člověk, jehož soukromí právo respektuje a chrání.[218] Posléze byla tedy věnována pozornost speciální úpravě chránící tato ve vztahu k zaměstnancům. Ve stejném duchu pak bylo nejprve obecně přiblíženo právo na ochranu majetku a následně možný výkon práva na ochranu majetku ve vlastnictví zaměstnavatele. Při rozboru relevantní úpravy byla vždy nejprve zohledněna mezinárodní právní úprava, včetně evropského právního rámce, a posléze české národní právní předpisy.

Pomyslným těžištěm práce pak byla kapitola věnovaná právě monitoringu zaměstnanců. V rámci ní byly přiblíženy a popsány jednotlivé právní tituly opravňující zaměstnavatele monitoring provádět. Dále se práce zaobírala důležitými povinnostmi a omezeními, které se k monitoringu váží, a konečně pak přišla řada na přiblížení a rozbor jednotlivých forem monitoringu. Za tímto účelem bylo vybráno několik významných soudních rozhodnutí, a to jak z české, tak zahraniční jurisdikce (včetně

[218] BĚLINA, M. a kol.: *Pracovní právo. 7. doplněné a podstatně přepracované vydání*. Praha: C. H. Beck, 2017, s. 166

rozhodnutí soudů evropských). V kapitole věnující se v krátkosti přiblížení právní úpravy zkoumané problematiky ve Velké Británii jsou pak pochopitelně zařazená i soudní rozhodnutí anglických soudů, která jsou případně i okomentována s poukazem na rozdílnost oproti české právní úpravě.

V rámci práce bylo na příslušných místech upozorněno na rozdílnost výkladů odborné veřejnosti, případně na ne vždy zcela konzistentní rozhodování soudů.[219] Nelze říct, že by důvodem byla nevhodně nastavená pravidla právní úpravy, nebo že by tato obsahovala závažné nedostatky. Vzhledem k tomu, že se z povahy věci musí jednat o úpravu s relativně neurčitou hypotézou, lze si jen stěží představit, a prakticky by to pak mohlo být spíše další komplikací, nějaké podrobné, až kazuistické nastavení pravidel a vytyčení hranic, kdy přesně je možné sledování provádět a kdy už nikoliv. V případě sledování zaměstnanců je totiž skutečně potřeba vždy posuzovat každé jedno sledovací opatření zvlášť a stejně tak konkrétní situaci, která k zavedení tohoto vedla. Jako důvod existence rozdílů ve výkladu autorka spatřuje spíše nedostatek vodítek (i pro samotné zaměstnavatele). Byť ÚOOÚ v tomto směru vydal několik stanovisek, porovnáte-li situaci s Velkou Británií, která je přiblížena v rámci 5. kapitoly, pak tamější zaměstnavatelé mají k dispozici téměř stostránkový dokument, a dále pak také další kodex věnovaný jen kamerovým systémům. Obsahem těchto jsou konkrétní rady a příklady pro zaměstnavatele, jak postupovat. V tomto směru tedy autorka nevnímá, ve vztahu k právní úpravě *de lege ferenda*, potřebu zásadně měnit textaci příslušných ustanovení, zejména tedy § 316 ZP.

Řešením *de lege ferenda*, které by přispělo k větší právní jistotě zaměstnavatelů, a potažmo i zaměstnanců, by podle autorky mohlo být poskytnutí autoritativních vodítek pro zavádění a provádění sledování v obdobné podrobnější publikaci. Pro tvorbu takové praktické příručky by mohly spojit síly ÚOOÚ a Státní úřad inspekce práce, neboť s účinností od 29. 7. 2017[220] jsou oba tyto úřady oprávněny udělovat zaměstnavatelům pokuty za porušení právních předpisů při provádění monitoringu. V tomto směru se jeví

[219] V této souvislosti je třeba znovu zmínit rozhodnutí ESLP ve věci Bărbulescu v. Rumunsko, stížnost č. 61496/08, kdy finální rozhodnutí senátu a velkého senátu jsou zcela opačná.

[220] Z důvodu novely ZIP publikované pod č. 206/2017 Sb.

současná publikace Státního úřadu inspekce práce, de facto dvoustranná, jako naprosto nedostatečná.[221]

Jako námět *de lege ferenda* lze jistě uvítat i podnět ke zpřesnění textace § 316 ZP, kdy by zaměstnancům mělo být zakázáno používat nejen pracovní prostředky ve vlastnictví zaměstnavatele, ale i ty, které zaměstnavatel zaměstnanci svěřil pro výkon práce a které si pouze pronajímá, stejně tak jako by se nemělo jednat pouze o konkrétní prostředky, ale například i zaměstnavatelem placené služby apod.[222] Ve stejném duchu lze obdobně navrhnout zpřesnění textace ve vztahu k informační povinnosti, kdy by tato i v ZP měla výslovně obsahovat povinnost informovat o účelu monitoringu (tedy nejen o způsobu a rozsahu kontroly), a dále by měla být zaměstnavateli přikázána ke splnění před započetím sledování, ve výjimečných situacích bezprostředně po provedení sledování (hrozilo-li by například, že zaměstnanec na základě informace o záměru monitorovat zničí důkazy, např. při šetření v rámci compliance programu by tak zaměstnavatel mohl přijít o cenné informace umožňující mu unést důkazní břemeno atd.).

Na vyhodnocenou aktuálnost této problematiky upozorňuje nejen probíhající legislativní vývoj, tedy např. přijetí nového nařízení o ochraně osobních údajů (GDPR), a dále nově připravovaný vládní návrh zákona o ochraně osobních údajů,[223] ale také zmíněná novela ZIP z roku 2017, která rozšířila oprávnění inspektorů (ve vztahu k ochraně soukromí zaměstnanců) udělovat zaměstnavatelům peněžité sankce namísto opatření k nápravě, ale také často zmiňovaný nepopiratelný technický pokrok a všudypřítomné skloňování zesilující potřeby ochrany soukromí jedinců, a to nejen na pracovišti, ale v životě celkově.

Při zaobíráním se tématem monitoringu zaměstnanců bylo potřeba brát v potaz jak pracovněprávní předpisy, tak předpisy o ochraně osobních údajů, neboť obě tato odvětví sledování zaměstnanců regulují a bez zohlednění obou naráz by pohled na sledování

[221] Publikace Státního úřadu inspekce práce *Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele*, dostupné online na WWW <http://www.suip.cz/_files/suip-7eb7366515abb7d99bf593cba68221bc/ochrana_os.pdf>

[222] PICHRT, J. a kol. *Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, s. 945

[223] Čj. OVA 55/18, sněmovní tisk č. 138/0, 8. volební období, od roku 2017, ve znění z 9. 4. 2018.

zaměstnanců nebyl komplexní. Vzhledem k tomu, že v práci pak byly taktéž zařazeny jak názory odborníků, tak soudů z konkrétních sporů, či dozorových orgánů, domnívá se autorka, že cíl diplomové práce přiblížit právní rámec a hranice legálnosti sledování zaměstnanců byl splněn.

Seznam nejčastěji použitých zkratek

AKV	Asociace kolektivního vyjednávání
DPA	the Data Protection Act 1998, zákon o ochraně osobních údajů účinný pro jurisdikci Anglie a Walesu
EPC	Employment Practices Code, kodex publikovaný Information Commisioner's Office poskytující informace a vodítka ke zpracování a zacházení s osobními údaji v rámci jurisdikce Anglie a Walesu
ESLP	Evropský soud pro lidská práva
EÚLP	Úmluva o ochraně lidských práv a základních svobod
GDPR	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)
ICO	Information Commisioner's Office, úřad Velké Británie s obdobnou působností jako český Úřad pro ochranu osobních údajů
Listina	Listina základních práv a svobod, vyhlášená zákonem č. 23/1991 Sb., kterým se uvozuje LISTINA ZÁKLADNÍCH PRÁV A SVOBOD jako ústavní zákon Federálního shromáždění České a Slovenské Federativní Republiky, republikovaná usnesením předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění ústavního zákona č. 162/1998 Sb., kterým se mění Listina základních práv a svobod
ObčZ	zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
Skupina WP29	Pracovní skupinu pro ochranu údajů zřízenou podle článku 29 Směrnice; jedná se o poradní orgán Evropské komise
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
ÚOOÚ	Úřad pro ochranu osobních údajů
ZIP	zákon č. 251/2005 Sb., o inspekci práce, ve znění pozdějších předpisů
ZOOÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
ZP	zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

Seznam použité literatury a zdrojů

Právní předpisy:

Listina základních práv a svobod, vyhlášená zákonem č. 23/1991 Sb., kterým se uvozuje LISTINA ZÁKLADNÍCH PRÁV A SVOBOD jako ústavní zákon Federálního shromáždění České a Slovenské Federativní Republiky, republikovaná usnesením předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění ústavního zákona č. 162/1998 Sb., kterým se mění Listina základních práv a svobod.

Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

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

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

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

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

Vyhláška ministra zahraničních věcí č. 120/1976 Sb., o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech.

Vyhlášky Státního úřadu pro jadernou bezpečnost č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu, v platném znění.

Návrh nového zákona o ochraně osobních údajů, čj. OVA 55/18, sněmovní tisk č. 138/0

Listina základních práv Evropské unie.

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

The Employments Right Act 1996 (Velká Británie)

The Data Protection Act 1988 (Velká Británie)

Regulation of Investigatory Powers Act 2000 (Velká Británie)

Bibliografie:

ANDRAŠČÍKOVÁ, M., HLOUŠKOVÁ, P. a kol. *Zákoník práce: prováděcí nařízení vlády a další související předpisy: s komentářem k 1. 1. 2016.* Olomouc: ANAG, 2016. Práce, mzdy, pojištění. 1272 s. ISBN 978-80-7263-992-2.

BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů: z pohledu zvláštních právních úprav k 1.8.2012*. Olomouc: ANAG, 2012. Právo (ANAG). 348 s. ISBN 978-80-7263-749-2.

BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. 304 s. ISBN 978-80-7552-141-5.

BĚLINA, M. PICHRT, J. a kol. *Pracovní právo*. 7., dopl. a podstatně přeprac. vyd. Praha: C.H. Beck, 2017. Academia iuris (C.H. Beck). 790 s. ISBN 978-80-7400-667-8.

BĚLINA, M. a kol. *Zákoník práce: komentář*. 2. vyd. Praha: C.H. Beck, 2015. Velké komentáře. 1613 s. ISBN 978-80-7400-290-8.

HŮRKA, P., ELIÁŠ, K. *Zákoník práce a související ustanovení občanského zákoníku: s podrobným komentářem k 1.1.2014*. 3., aktualiz a rozš. vyd. Olomouc: ANAG, 2014. 1063 s. ISBN 978-80-7263-85-4.

JANEČKOVÁ, E., BARTÍK, V. *Kamerové systémy v praxi: Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde, 2011. 240 s. ISBN 978-80-7201-850-5.

KUČEROVÁ, A. a kol. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. 536 s. ISBN 978-80-7179-226-0.

MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). 436 s. ISBN 978-80-7478-139-1.

NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). 504 s. ISBN 978-80-7478-665-5.

ŠTEFKO, M., VYSOKAJOVÁ., M. *Personální vademecum*. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2016. 98 s. ISBN 978-80-879-75-45-9.

PICHRT, J. a kol. *Zákoník práce: Zákon o kolektivním vyjednávání*. Praha: Wolters Kluwer, 2017. Praktický komentář. 1196 s. ISBN 978-80-7552-609-0.

VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer. Právní aspekty monitoringu zaměstnanců*. 1. vydání. Praha: C.H. Beck, 2013. Beckova edice ABC. 249 s. ISBN 978-80-7400-453-7.

WAGNEROVÁ, E., ŠIMÍČEK, V. a kol. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer Česká republika, 2012. Komentáře (Wolters Kluwer ČR). 906 s. ISBN 978-80-7357-750-6.

DEAKIN, S., MORRIS, G. *Labour Law.* 6. vydání. Portland, Oregon: Hart Publishing, 2012. 1360 s. ISBN 978-1849463416.

COLLINS, H., EWING, K.D., a McCOLGAN, A. *Labour Law: Text and Materials.* 2. vydání. Portland, Oregon. Hart Publishing, 2005. 1168 s. ISBN 978-1841133621.

HONEYBALL, S. *Honeyball & Bowers' textbook on employment law*. 13. vydání. New York, NY: Oxford University Press, 2014. 528 s. ISBN 978-0199685622.

Odborné články:

BOND, R., PROTOKOVA, V. Monitoring in the workplace - damned if you do and damned if you don't! *Compliance & Risk,* 2015, **4**(3).

JOUZA, L. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. *Bulletin advokacie*. 2014, **21**(6).

KADLECOVÁ, T. GPS ve služebních vozidlech aneb malý čip = velká komplikace? *Praktická personalistika*, 2015, **1**(3-4).

MORÁVEK, J. Sledování zaměstnanců v kontextu novely zákoníku práce. *Právní rozhledy.* 2012, **20**(5).

NONNEMANN, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, **23**(7).

RADIČOVÁ, Z. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy.* 2014 **22(**21).

SAKROUGE, A., a kol. Monitoring employee communications: data protection and privacy issues. *C.T.L.R*. 2011, **17**(8).

ŠTEFKO, M. K problému sledování vlastních zaměstnanců. *Právo a zaměstnání*. 2015, **11**(1).

TOMŠEJ, J., METELKA, J. *Ochrana soukromí nad zlato.* Server https://www.epravo.cz. Dostupné online na WWW <https://www.epravo.cz/top/clanky/ochrana-soukromi-nad-zlato-92358.html> [cit. 29.4.2018].

VALENTOVÁ, K. Jak legálně sledovat zaměstnance. *Právní rádce*. 2016, **23**(7-8).

ZEMANOVÁ ŠIMONOVÁ, H. Právní prostředky ochrany osobnosti zaměstnance. *Bulletin advokacie*. 2016, **23**(10).

[Autor neuveden]. Subject access request by employees – 2. *IDS Emp. L. Brief* 2015, 1025.

Judikatura:

Rozhodnutí ESLP ve věci Antović a Mirković v. Černá Hora ze dne 28. 11. 2017 (konečné znění ze dne 28. 2. 2018), stížnost č. 70838/13

Rozhodnutí ESLP ve věci Niemietz v. Německo ze dne 16. prosince 1992, stížnost č. 13710/88

Rozhodnutí ESLP ve věci Halford v. Velká Británie ze dne 26. června 1997, stížnost č. 20605/92

Rozhodnutí ESLP ve věci Copland v. Velká Británie ze dne 3. 4. 2007 (konečné znění ze dne 3. 7. 2007), stížnost č. 62617/00

Rozhodnutí ESLP ve věci Bărbulescu v. Rumunsko, stížnost č. 61496/08

Nález Ústavního soudu ČR II. ÚS 1774/14 ze dne 9. 12. 2014

Nález Ústavního soud ČR Pl. ÚS 4/94 ze dne 12. 10. 1994, publikováno pod č. 214/1994 Sb., nebo také nález Ústavního soudu ČR Pl. ÚS. 3/02 ze dne 13. 8. 2002, publikováno pod č. 405/2002 Sb

Nález Ústavní soudu ČR sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001

Usnesení Ústavního soudu ČR I. ÚS 3933/12 ze dne 7. 11. 2012

Rozsudek Nejvyšší správní soud ČR sp. zn. 9 As 34/2008 ze dne 12. 2. 2009

Rozsudek Nejvyššího soudu ČR sp. zn. 11 Tdo 349/2009, ze dne 21.5.2009, publikováno pod T 1197 v Souboru trestních rozhodnutí a stanovisek Nejvyššího soudu ČR

Rozsudek Nejvyššího soudu ČR sp. zn. 21 Cdo 1009/98 ze dne 21. 10. 1998, publikován ve Sbírce soudních rozhodnutí a stanovisek pod č. R 39/99

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

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

Rozsudek Nejvyššího správního soudu ČR sp.zn. 5 As 1/2011 - 156 ze dne 28. 6. 2013

Rozsudek Nejvyššího správního soudu ČR sp. zn. 10 As 245/2016 – 41 ze dne 20. 12. 2017

Rozsudek Městského soudu v Praze, sp. zn. 5 A 107/2013 – 38 ze dne 18. 10. 2016

Rozsudek Městského soudu v Praze sp. zn. 6 A 42/2013 – 48 ze dne 5. 5. 2017

Eric Morris v. Ford Motor Company [1973] EWCA Civ J0327-1

Malik v Bank of Credit and Commerce International SA (In Liquidation) [1997] I.C.R. 606

Elliott v Lloyds TSB Bank Plc & Anor [2012] EW Misc 7

McGowan v Scottish Water [2005] IRLR 167

Důvodové zprávy:

Důvodová zpráva k návrhu ZP, sněm. tisk 1153/0, ze 4. období Poslanecké sněmovny (2002 – 2006)

Důvodová zpráva k návrhu ZOOÚ, sněm. tisk 374/0, ze 3. období Poslanecké sněmovny (1998 – 2002)

Elektronické zdroje a ostatní:

Sněmovní tisk č. 428 ze 6. období Poslanecké sněmovny (2010 – 2013)

Stanovisko vlády, sněmovní tisk č. 428/1, ze 6. období Poslanecké sněmovny (2010 – 2013)

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

Stanovisko ÚOOÚ č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště

Stanovisko ÚOOÚ č. 3/2009 – Biometrická identifikace nebo autentizace zaměstnanců, aktualizované skrze stanovisko ÚOOÚ č. 1/2017

Stanovisko ÚOOÚ č. 6/2009 – Ochrana soukromí při zpracování osobních údajů

Stanovisko ÚOOÚ č. 6/2012 – Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů

Stanovisko ÚOOÚ č. 3/2014 – K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti

Stanovisko ÚOOÚ č. 1/2015 - Provozování kamery v motorovém vozidle se záběrem mimo toto vozidlo

Zápis z jednání Kolegia expertů AKV konaného v Kolíně ve dnech 3. a 4. 11. 2017

Výkladová stanoviska AKV (XIX.), přijatá na zasedání Kolegia expertů AKV v Kolíně ve dnech 4. a 5. 11. 2016 – IV. část, část 24 a 27

Stanovisko Skupiny WP29 č. 2/2017, "*Opinion on data processing at work*", dostupné online na WWW <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169>,

Tisková zpráva ÚOOÚ ze dne 1. 3. 2018: „*S účinností GDPR končí oznamovací povinnost správců*", dostupná online na WWW <https://www.uoou.cz/s-nbsp-ucinnosti-gdpr-konci-oznamovaci-povinnost-spravcu/d-28855>,

Publikace Státního úřadu inspekce práce *Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele*, dostupné online na WWW <http://www.suip.cz/_files/suip-7eb7366515abb7d99bf593cba68221bc/ochrana_os.pdf>

Sdělení ÚOOÚ vydané dne 13. března 2018, dostupné online na WWW: <https://www.uoou.cz/upozorneni-na-zmenu-v-nbsp-posuzovani-systemu-vyuzivajicich-biometricke-udaje-drive-quot-stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu-quot/d-29048/p1=2247

Stanovisko Skupiny WP29 č. 4/2004, „*Ke zpracování osobních údajů prostředky kamerového sledování*", dostupné online na WWW <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22427>

Sdělení Evropské komise "*Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection*", ze dne 9. ledna 2018, dostupné online na WWW <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=611943>,

The Employment Practices Code on Data Protection, dostupný online na WWW <https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf>

Publikace *An overview of UK data protection law*, dostupná online na WWW <https://united-kingdom.taylorwessing.com/uploads/tx_siruplawyermanagement/NB_000168_Overview_UK_data_protection_law_WEB.pdf>,

CCTV Code of Practice, dostupný online na WWW <https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

Monitoring zaměstnanců

Abstrakt

Tématem předmětné diplomové práce je, jak název sám napovídá, monitoring zaměstnanců. S neustálým vývojem a pokrokem technologických možností a jejich dostupnosti je soukromí člověka potenciálně čím dál tím více ohroženo, tím spíše pak soukromí zaměstnance na pracovišti, kdy má zaměstnavatel nepřeberné možnosti a prostor sledovat jej a jeho činnost na pracovišti, leckdy pak i mimo něj. Na druhou stranu lze pochopit i úmysl zaměstnavatele chránit svůj majetek a finanční prostředky, které investuje do provozu svého podnikání.

Zvolené téma tedy nabízí prostor pro hodnocení střetu dvou práv, kdy na sebe naráží právo na ochranu soukromí a právo na ochranu majetku. Z tohoto důvodu bere celá práce v potaz jak pracovněprávní předpisy, tak předpisy upravující ochranu osobních údajů, které mohou být monitoringem ohroženy. S ohledem na blížící se účinnost nařízení (EU) 2016/679 je na vybraných místech v krátkosti zmíněno i toto, zejména při hodnocení, zda lze v dané oblasti do budoucna očekávat změny, či nikoliv.

Práce je členěna do šesti kapitol včetně úvodu a závěru. Úvodní kapitola blíže přibližuje rozsah zkoumané problematiky a aktuálnost tématu. Druhá kapitola této práce se zaobírá mezinárodním i českým právním rámcem ochrany soukromí člověka a dále zaměstnance. Následující třetí kapitola při stejném postupu přibližuje právní úpravu ochrany vlastnictví a majetku – opět nejprve obecně a posléze majetku zaměstnavatelove. Náplní čtvrté kapitoly je pak samotný monitoring zaměstnanců. Nejprve jsou obecně přiblíženy různé formy sledování zaměstnanců, následně zákonné důvody umožňující legální monitoring. Text se pak dále zaobírá relevantními povinnostmi a omezeními, které zaměstnavatel musí při sledování zaměstnanců dodržovat a respektovat a posléze již práce přechází k přiblížení konkrétních vybraných způsobů sledování zaměstnanců. Zde se práce blíže věnuje rozboru judikatury, neb konkrétní rozhodnutí soudů nejlépe demonstrují, jaký monitoring obstojí před zákonem a jaký již nikoliv. V práci jsou zařazeny rozhodnutí jak soudů českých, tak i rozhodnutí Evropského soudu pro lidská práva. Pátá kapitola cílí na krátké uvedení do zkoumané problematiky v rámci jurisdikce Anglie a Walesu a následně

vybírá zajímavé odlišnosti při porovnání s českou úpravou. Pochopitelně i zde se práce věnuje judikatuře, a to samozřejmě judikátům soudů anglických.

Cílem práce bylo sumarizovat relevantní právní úpravu a vedle toho diskutovat hranice možností legálního monitoringu zaměstnanců.

Klíčová slova: monitoring zaměstnanců, ochrana soukromí, majetek zaměstnavatele

Monitoring of employees

Abstract

The theme of this diploma thesis is, as the title suggests, the monitoring of employees. With the continuous development and progress of technologies and their increasing availability, the privacy of citizens is becoming increasingly more endangered. Even more concerning is the privacy of employees in the workplace, where an employer has inexhaustible possibilities to monitor activity at work - and sometimes outside of the workplace as well. On the other hand, the intention of the employer to protect its assets and the financial means invested in the operation of its business is appreciable and in some ways necessary to align with the employer's obligations to their shareholders.

Therefore, the chosen subject brings to the surface the conflict of two equal rights, as the right to protection of privacy collides with the right of protection of property. For this reason, the whole thesis takes into account both the labour law regulations and the regulations on the protection of personal data - since personal data of employees can be threatened by monitoring. With regard to the fact, that Regulation (EU) 2016/679 comes into effect soon, it is briefly mentioned in the relevant parts, especially when assessing whether it will impact the legal interpretation in the future or not.

The thesis is divided into six chapters, including the introduction and conclusion. The introductory chapter describes the scope of the subject and how the inherent tension between rights manifests itself. The second chapter is devoted to both the international and Czech legal frameworks on the protection of privacy, and then the further privacy of employees. The third chapter introduces (with the same approach) the general legal regulation on the protection of property, and then further the protection of employers' assets.

The fourth chapter is dedicated to the monitoring of employees itself. Firstly, the various forms of monitoring are discussed, followed by statutory reasons for legal monitoring. It will then address the relevant obligations and limitations the employer has to observe and respect when monitoring its employees, as well as investigating the specific selected monitoring methods seen. Here, the work closely analyses the courts' decisions, since particular decisions demonstrate best which forms of monitoring might be still deemed

legal and which are not. Included are decisions of the Czech courts and decisions of the European Court of Human Rights as well.

The fifth chapter aims to briefly introduce the reader to the subject through the legislation of the United Kingdom and subsequently draws attention to interesting differences when compared with Czech legislation. Of course, British case law is mentioned and discussed in this chapter as well.

The aim of the thesis is to summarize the relevant legal frameworks and legislation, and to explore the limits of legitimate and legal monitoring of employees.

Klíčová slova: monitoring of employees, protection of privacy, employer's assests