UNIVERZITA KARLOVA V PRAZE
PRÁVNICKÁ FAKULTA

Mgr. Petra Zůnová

MONITORING ZAMĚSTNANCŮ A JEHO METODY

Rigorózní práce

Vedoucí rigorózní práce: doc. JUDr. Martin Štefko, Ph.D.
Katedra pracovního práva a práva sociálního zabezpečení
Datum vypracování práce (uzavření rukopisu): 14. listopadu 2017

PROHLÁŠENÍ

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

V Praze dne _____

Mgr. Petra Zůnová

PROHLÁŠENÍ O POČTU ZNAKŮ

Vlastní text rigorózní práce včetně poznámek pod čarou má celkem 294 414 znaků.

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala především doc. JUDr. Martinu Štefkovi, Ph.D., za cenné připomínky a rady při vypracování této rigorózní práce.

Obsah

Seznam zkratek

AML Zákon	zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu;
EDPS	Evropský inspektor ochrany údajů (v originále: „*European Data Protection Supervisor*“);
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);
OZ	zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů;
Pracovní skupina	pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená na základě čl. 29 Směrnice 95/46/ES;
Sbor	Evropský sbor pro ochranu osobních údajů, jenž má být zřízen dle čl. 68 odst. 1 GDPR;
Směrnice 95/46/ES	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;
SŘ	zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů;
TOPO	zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.
TZ	zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů;
ÚOOÚ	Úřad pro ochranu osobních údajů;
zákon o hazardních hrách	zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů;
zákon o inspekci práce	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;
ZOP	zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich;
ZP	zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

Úvod

Fenoménem dnešní doby jsou moderní komunikační prostředky a informační technologie, bez nichž si většina z nás již ani neumí svět představit. Staly se běžnou součástí nejen našeho soukromého života, ale postupně též toho pracovního. Podstatná část dnešních zaměstnanců komunikuje prostřednictvím pracovní e-mailové schránky a k práci využívá služební počítač a mobilní telefon (čím dál častěji smartphone). Moderní komunikační prostředky a informační technologie zrychlují výměnu informací prakticky po celém světě a zefektivňují práci. Umožňují zaměstnancům nové, flexibilnější, způsoby výkonu práce, ať už v podobě tzv. teleworkingu, nebo práce z domova, a zaměstnavatelům přinášejí nové možnosti v oblasti řízení zaměstnanců a organizace práce, jakož i zvyšování její efektivity.

Na druhou stranu ovšem používání moderních komunikačních prostředků a informačních technologií v pracovněprávních vztazích přináší řadu výzev, jimž je třeba čelit. Zaměstnavatelé jsou vystavováni mnoha rizikům, mezi něž patří zejména zneužití či únik informací, ohrožení či zničení dat, ztráta know-how nebo ohrožení dobrého jména, k nimž nyní může dojít mnohem snadněji, a to také nedbalostním či dokonce úmyslným jednáním zaměstnance. Ve snaze těmto rizikům zamezit přijímají zaměstnavatelé řadu bezpečnostních opatření včetně sledování a pravidelné kontroly zaměstnanců. Tím však narážejí na ústavně zaručené právo zaměstnanců na soukromí. A nejen na to; podrobení zaměstnance detailnímu dohledu nad jeho aktivitami v práci může vést k narušení jeho důvěry a loajality vůči zaměstnavateli, které jsou klíčem k oboustranné spokojenosti v daném pracovněprávním vztahu.

Kde tedy nalézt rovnováhu mezi ochranou zaměstnavatelů, zejména jejich práva na ochranu majetku, nerušenou podnikatelskou činnost a dobrou pověst, a ochranou zaměstnanců před nepřiměřeným zasahováním do soukromí? V praxi bývá často poměrně obtížné nalézt správné řešení, v jehož rámci by nepřiměřeně nebyla upřednostňována práva jedné strany na úkor druhé. Cílem této práce je poskytnout vhled do této problematiky a zároveň navrhnout určitá řešení konkrétních situací.

Tato práce je tematicky rozdělena do tří hlavních částí. První její část se zabývá obecnými podmínkami, za nichž je zaměstnavatel oprávněn k ochraně svých práv a právem chráněných zájmů zavést opatření určená ke sledování zaměstnanců. Tyto

podmínky vycházejí v prvé řadě z úpravy ZP, ovšem bude-li monitoring zároveň představovat zpracování osobních údajů zaměstnanců (jak tomu ve většině případů skutečně bude), bude nezbytné plnit též řadu dalších podmínek stanovených v právních předpisech týkajících se ochrany osobních údajů. V době odevzdání této práce stále platí ZOOÚ; zároveň však byl na úrovni Evropské unie po dlouholetých přípravách přijat klíčový právní předpis na poli ochrany osobních údajů, a sice GDPR. Tímto nařízením dojde ke zrušení stávající Směrnice 95/46/ES, jež byla do českého právního řádu implementována právě prostřednictvím ZOOÚ. Oficiální projednávání GDPR započalo již v roce 2012, tj. jeho přípravy probíhaly ještě dříve, a trvalo až do 27. dubna 2016, kdy bylo vydáno. Od té doby toto nařízení vyvolává nejen mezi odbornou veřejností, ale především mezi podnikatelskými subjekty neobvyklou vlnu emocí a zejména obav ze zásadního zpřísnění nakládání s osobními údaji.

Zpravidla je GDPR zejména ve sdělovacích prostředcích označováno doslova za revoluci v oblasti ochrany osobních údajů. Toto nařízení skutečně správcům a zpracovatelům osobních údajů přináší řadu nových povinností s deklarovaným cílem jejich důsledného vymáhání za účelem vyšší úrovně ochrany subjektů údajů. Dle úvodních recitálů tím reaguje na bouřlivý technologický vývoj, který od vydání Směrnice 95/46/ES proběhl a v jehož důsledku jsou osobní údaje stále více využívány, což pochopitelně přináší také zvýšená rizika jejich zneužití.[1] Aby byla zajištěna jednotná úprava v zásadních otázkách ochrany osobních údajů, byla zvolena forma přímo použitelného nařízení. Předchozí úprava pomocí Směrnice 95/46/ES byla v tomto směru údajně nevyhovující, neboť vzhledem k různým podobám její harmonizace docházelo stále ke značným rozdílům úrovně ochrany osobních údajů napříč členskými státy. Tento stav je dle tvůrců nové normy zejména s ohledem na rostoucí přeshraniční pohyb osobních údajů nežádoucí.[2] Na druhou stranu, GDPR se výslovně hlásí k cílům a zásadám předchozí Směrnice 95/46/ES, tj. k principu kontinuity.[3] Jak proto v této

1 Viz recitál 6 GDPR.

2 Viz recitál 9, 10 a 13 GDPR.

3 Viz recitál 9 GDPR.

souvislosti upozorňuje ÚOOÚ, není zcela na místě jej označovat za revoluční právní úpravu.[4]

GDPR má ovšem také celou řadu kritiků. Jak např. upozorňuje Morávek, údajná zastaralost „předinternetové" Směrnice 95/46/ES nemusela nutně vést k jejímu zrušení. Plně by postačilo její doplnění v návaznosti na potřeby aplikační praxe (zejména v oblasti přeshraničního předávání osobních údajů včetně jejich předávání v rámci nadnárodních korporací) s tím, že zbylé problematické otázky by jistě bylo možné vzhledem k jejímu poměrně obecnému textu překlenout výkladem či prostřednictvím dotváření práva. Morávek rovněž kritizuje zvolenou formu nařízení, která je dle jeho názoru v rozporu se zásadou subsidiarity, kterou stanoví čl. 5 odst. 3 Smlouvy o Evropské unii.[5] Konstatuje, že deklarovaný cíl, tj. odstranění rozdílného uplatňování pravidel v oblasti ochrany osobních údajů v jednotlivých členských státech, jímž je právě volba nařízení odůvodněna, nebude dosažitelný ani po účinnosti GDPR.[6] Důvod je prostý; GDPR bude v každém jednotlivém členském státě aplikováno místními dozorovými úřady, jejichž kompetence a personální vybavenost se stát od státu liší. Další výklad této normy pak budou provádět národní soudy, které tak samozřejmě budou ovlivňovat praxi příslušného dozorového úřadu.[7] Jednotnou judikaturu a přístup dozorových úřadů na úrovni všech členských států pochopitelně očekávat nelze, a proto je tato kritika zcela na místě.

GDPR pochopitelně zasáhne též problematiku monitoringu zaměstnanců, bude-li při něm docházet ke zpracování jejich osobních údajů. S ohledem na blížící se účinnost tohoto nařízení, jež nastane 25. května 2018, proto v problematice ochrany osobních údajů vycházím jak ze ZOOÚ, tak ze znění a dostupných výkladů GDPR. Přesto se tato práce pohybuje ve stavu určitého vakua, neboť na úrovni českého práva má

---

[4] ÚOOÚ: Desatero omylů o obecném nařízení (GDPR) [online]. Publikováno dne 25. května 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/desatero-omylu-o-obecnem-narizeni-gdpr/d-23799/p1=3938>.

[5] Znění čl. 5 odst. 3 Smlouvy o Evropské unii: „*Podle zásady subsidiarity jedná Unie v oblastech, které nespadají do její výlučné pravomoci, pouze tehdy a do té míry, pokud cílů zamýšlené činnosti nemůže být dosaženo uspokojivě členskými státy na úrovni ústřední, regionální či místní, ale spíše jich, z důvodu jejího rozsahu či účinků, může být lépe dosaženo na úrovni Unie*."

[6] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, dostupné elektronicky v systému ASPI, Část III., kapitola 2. ISBN 978-80-7478-139-1.

[7] Tamtéž, Část III., kapitola 2.2.

k legislativním změnám souvisejícím s účinností GDPR teprve dojít. Nařízení bude samozřejmě přímo použitelné, ať už český zákonodárce stihne včas připravit aktualizovaný národní právní předpis či nikoli. Pravděpodobně nebude zvolena cesta novelizace ZOOÚ, jež by s ohledem na značné množství změn byla velmi nepřehledná, ale vydání zcela nového předpisu. Tento scénář ostatně naznačilo Ministerstvo vnitra České republiky, když dne 18. srpna 2017 předložilo k připomínkám návrh zbrusu nového zákona o zpracování osobních údajů. Stalo se tak ovšem těsně před říjnovými volbami do Poslanecké sněmovny Parlamentu České republiky, tudíž je otázkou, zda bude návrh předložen ve stejné podobě i nově sestavenou vládou. Ještě větší otázkou je pak pochopitelně osud návrhu v rámci legislativního procesu.

Cenným zdrojem výkladů v oblasti problematiky ochrany osobních údajů na unijní úrovni jsou (právně nezávazná) stanoviska Pracovní skupiny coby nezávislého orgánu zřízeného dle čl. 29 Směrnice 95/46/ES.[8] Pokud na ně tato práce odkazuje, činí tak pouze v případě, kdy budou nadále použitelná i dle GDPR s ohledem na obdobné znění Směrnice 95/46/ES, ledaže je výslovně uvedeno jinak.

Těžištěm této práce je její druhá část, která se již věnuje konkrétním metodám monitoringu zaměstnanců. Podrobně jsou rozebrány ty metody, s nimiž se lze na pracovištích setkat nejčastěji, tj. kontrola elektronické pošty, kontrola činnosti zaměstnanců na internetu, kamerové systémy, monitoring pomocí GPS a monitoring užívání služebních telefonů. Pro tyto metody popisuji též jejich konkrétní scénáře, které by bylo možné dle mého názoru v praxi zavést, samozřejmě při splnění obecných podmínek monitoringu rozebraných v první části této práce. Uvádím nicméně i další vybrané a méně časté metody monitoringu, konkrétně monitoring docházky a vstupů do zabezpečených prostor pomocí biometrických údajů, monitoring užívání služebního počítače a práce se soubory, monitoring tiskových úloh a tzv. *mystery shopping*. Samozřejmě existují také další metody monitoringu, některé z nich však zasahují do soukromí zaměstnanců natolik nepřiměřeně, že by jejich využití za dané právní úpravy

[8] Pracovní skupina byla zřízena za účelem poskytování poradenství Evropské komisi v oblasti ochrany osobních údajů a přispívání k jednotnému provádění vnitrostátních předpisů přijatých na základě uvedené směrnice. S účinností GDPR, které Směrnici 95/46/ES v plném rozsahu ruší, bude Pracovní skupina nahrazena Sborem, jemuž GDPR výslovně přiznává právní subjektivitu a který má mít oproti Pracovní skupině mnohem širší pravomoci (viz čl. 70 GDPR ve srovnání s čl. 30 Směrnice 95/46/ES).

možná připadalo v úvahu pouze u velmi specifických zaměstnavatelů (např. tajné služby, armáda). Mezi tyto prostředky patří např. *keylogging* (software zaznamenávající veškeré stisknuté klávesy na počítači a detailní pohyb kurzoru) nebo *sniffing* (software umožňující odposlouchávání datové komunikace na počítači).

U každé metody monitoringu jsou též detailně rozebrány dostupné případy řešené v rámci relevantní rozhodovací praxe, a to jak na úrovni Evropského soudu pro lidská práva, jenž bdí nad dodržováním práva na ochranu soukromí garantovaného v čl. 8 Úmluvy o ochraně lidských práv a základních svobod i v pracovněprávních vztazích, tak na úrovni ÚOOÚ a českých soudů. Tato rozhodovací praxe však není s výjimkou problematiky kamerových systémů příliš hojná, přestože pro monitoring klíčové ustanovení § 316 ZP je v českém právním řádu zakotveno v nenovelizované podobě již od 1. ledna 2007.

Konečně ve třetí části této práce se zabývám tématy, která s monitoringem zaměstnanců úzce souvisejí. Patří sem na jedné straně možnosti zaměstnavatele sledovat pomocí monitoringu též pracovní výkonnost zaměstnanců a vyvozovat z výsledků monitoringu vůči konkrétním zaměstnancům pracovněprávní důsledky, na straně druhé prostředky právní obrany zaměstnanců proti monitoringu. Nastíněna je též problematika BYOD (z anglického „*Bring Your Own Device*“) s ohledem na monitoring, tj. řešení, kdy zaměstnanci se souhlasem zaměstnavatele užívají svá soukromá zařízení též k výkonu práce.

Zatímco zaměstnavatelé mají často tendenci zaměstnance sledovat více, než je pro ochranu jejich zájmů skutečně nutné, zaměstnanci zpravidla vnímají každý, a to i z právního pohledu přiměřený, monitoring velmi negativně. Tato práce si proto přeje nabídnout vyvážený právní náhled na problematiku sledování zaměstnanců z pohledu obou stran. Ambicí této práce však není popis technické stránky jednotlivých metod monitoringu.

1. Předpoklady monitoringu zaměstnanců

1.1 Právo zaměstnanců na soukromí

Právo na soukromí patří mezi základní lidská práva zakotvená v celé řadě mezinárodních smluv[9]. Nedotknutelnost soukromí každé osoby zakotvuje v českém ústavním právu článek 7 Listiny základních práv a svobod, podle něhož ji lze omezit pouze v případech stanovených zákonem. Konkrétněji pak ochranu soukromí každého člověka a jeho práva vyplývající z neoprávněného zásahu do soukromí rozvádí OZ v § 81 a násl. Klíčové je v tomto směru především ustanovení § 86 OZ: „*nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.*“ Zároveň však musí každý zásah do soukromí člověka projít testem principu proporcionality (§ 90 OZ), tj. nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka (viz k tomu podrobný výklad v kapitole 1.3. níže).

Není jistě pochyb o platnosti výše uvedených principů v rámci ryze soukromého života každého člověka. Do jaké míry je však třeba je aplikovat i v pracovněprávních vztazích? Touto otázkou se zabýval Evropský soud pro lidská práva např. ve věci Niemietz proti Německu při posuzování skutečnosti, zda prohlídka advokátní kanceláře pana Niemietze provedená ze strany orgánů činných v trestním řízení byla zásahem do jeho práva na nedotknutelnost obydlí, přestože se jednalo o prostory, v nichž pan Niemietz provozoval svou advokátní praxi, a nikoli o obydlí jako takové (pomiňme v tomto kontextu problematiku prohlídek prostor, v nichž dochází k výkonu advokacie, ze strany orgánů činných v trestním řízení, která je v českém právu řešena specificky). Soud konstatoval, že pojem „soukromý život“ nelze omezovat pouze „*na „vnitřní kruh“, v jehož rámci může jednotlivec žít svůj vlastní osobní život podle libosti, a zcela z něho vyloučit vnější svět nezahrnutý do tohoto kruhu*“, když právo na soukromí musí do jisté

[9] Zejména čl. 12 Všeobecné deklarace lidských práv, čl. 17 Mezinárodního paktu o občanských a politických právech, čl. 8 Úmluvy o ochraně lidských práv a základních svobod a čl. 16 Smlouvy o fungování Evropské unie (zde je přímo zakotveno právo každého na ochranu osobních údajů, které se jej týkají).

míry zahrnovat také právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi. K rozvíjení takových vztahů samozřejmě dochází nevyhnutelně rovněž během pracovní činnosti, přičemž není možné vždy jasně rozlišit, které činnosti jednotlivce tvoří část jeho profesního nebo obchodního života a které nikoli.[10] Obdobně Evropský soud pro lidská práva přiznal zaměstnancům právo na ochranu soukromí v případě telefonátů uskutečněných na pracovišti zaměstnavatele[11] a také v případě odeslaných e-mailů a informací ohledně používání internetu pro soukromé účely (obojí během pracovní doby a na pracovišti zaměstnavatele).[12] V obou zmíněných případech soud zdůraznil legitimní očekávání zaměstnanců ohledně zachování jejich soukromí na pracovišti v situaci, kdy bylo užívání pracovních prostředků pro soukromé účely dovoleno nebo alespoň fakticky tolerováno. Naopak toto legitimní očekávání zaměstnance a jeho právo na ochranu soukromí neuznal v případě, kdy zaměstnanec využil pracovní prostředky zaměstnavatele pro soukromé účely přes jeho výslovný předchozí zákaz.[13]

Výše uvedené výklady Evropského soudu pro lidská práva se sice mohou z pohledu zaměstnavatele zdát poměrně široké, jsou však vcelku realistické. Zaměstnanci neodkládají své právo na soukromí a ochranu osobních údajů každý den u vstupu na pracoviště.[14] Ve chvíli, kdy zaměstnanec tráví většinu aktivního dne v práci, nelze očekávat (a po zaměstnanci ani rozumně požadovat), že ani na okamžik nesklouzne k řešení vlastních soukromých záležitostí, nebo že nebude navazovat jiné než ryze pracovní kontakty s ostatními zaměstnanci, případně též se zákazníky zaměstnavatele. Jistě je i v zájmu zaměstnavatele, aby k takovým kontaktům v rozumné míře (a na korektní úrovni) docházelo, neboť se tím nepochybně posiluje vzájemná důvěra mezi zaměstnanci, potažmo mezi zaměstnanci a zákazníky zaměstnavatele, kolegialita a týmová práce, přičemž v konečném důsledku mohou zaměstnanci pracovat i mnohem

---

10 Rozsudek Evropského soudu pro lidská práva, stížnost č. 13710/88, ze dne 16. prosince 1992, Věc Niemietz versus Německo.

11 Např. rozsudek Evropského soudu pro lidská práva, stížnost č. 20605/92, ze dne 25. června 1997, Věc Halfordová proti Spojenému království.

12 Např. rozsudek Evropského soudu pro lidská práva, stížnost č. 62617/00, ze dne 3. dubna 2007, Věc Coplandová proti Spojenému království.

13 Rozsudek Evropského soudu pro lidská práva, stížnost č. 61496/08, ze dne 12. ledna 2016, Věc Bărbulescu proti Rumunsku.

14 Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Pracovní dokument o sledování elektronických komunikací na pracovišti (v originále: „*Working document on the surveillance of electronic communications in the workplace*“) ze dne 29. května 2002, s. 4.

efektivněji, než kdyby jim byly tyto aktivity zapovězeny. Příjemné pracovní prostředí a atmosféra též zpravidla snižují fluktuaci zaměstnanců, a tím logicky náklady zaměstnavatele na hledání a zaučování nových. Ostatně socializační aspekt závislé práce si přál vyjádřit i zákonodárce v návrhu nového znění § 317 odst. 4 ZP[15], podle něhož měl být zaměstnavatel povinen zajistit zaměstnanci pracujícímu mimo jeho pracoviště na jeho žádost kontakt s ostatními zaměstnanci a možnost se s nimi pravidelně osobně setkávat na pracovišti zaměstnavatele. Tato změna však nakonec přijata nebyla, neboť Poslanecká sněmovna Parlamentu České republiky v 7. volebním období nestihla předmětnou novelu zákoníku práce projednat.

Na druhou stranu, soukromí na pracovišti má své meze. Jak vyjádřil Ústavní soud, „*právo na ochranu před neoprávněnými zásahy do soukromí se zpravidla vztahuje na případy zásahů do soukromé a rodinné sféry, v nichž jednotlivec projevuje svou osobnost svobodně a autonomně. V této sféře se však neocitá za situace, kdy v prostředí zaměstnavatele vystupuje a plní funkce pracovního charakteru. Rovněž pak listovní tajemství, tajemství jiných písemností a záznamů, tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením, nelze vztahovat na činnost, která má být svou povahou činností pracovní*.“[16]

1.2 Právo zaměstnavatele na ochranu majetku a dalších hodnot

Proti právu zaměstnanců na ochranu soukromí při práci stojí na druhé straně právo zaměstnavatele vlastnit majetek a ochraňovat jej před zásahy ostatních, rovněž zaručené mezinárodními smlouvami a ústavním pořádkem.[17] Cílem většiny zaměstnavatelů je zásadně efektivní dosahování zisku, respektive provádění vlastní (byť nevýdělečné) činnosti, v každém případě však zachování majetkových hodnot, které zaměstnavatel ke své činnosti používá a k nimž mají jeho zaměstnanci z titulu svého pracovního zařazení přístup. Nejde pouze o ochranu hmotného majetku; v době digitálních technologií a internetu nabývá na důležitosti především ochrana nehmotného majetku (práv

[15] Novela zákoníku práce (sněmovní tisk č. 903/0), projednávaná v Poslanecké sněmovně Parlamentu České republiky v 7. volebním období (2013 – 2017).

[16] Usnesení Ústavního soudu sp. zn. I. ÚS 452/09 ze dne 31. března 2009.

[17] Zejména čl. 17 Všeobecné deklarace lidských práv, čl. 1 Dodatkového protokolu k Úmluvě o ochraně lidských práv a základních svobod a čl. 11 Listiny základních práv a svobod.

duševního vlastnictví), know-how a informací. Laicky řečeno, ukrást data může být jednodušší a přitom mít dalekosáhlejší následky než ukrást zaměstnavateli zboží ze skladu. Kromě toho, že ztráta nehmotného majetku, důležitých dat, informací a know-how může vést k zásadnímu narušení činnosti zaměstnavatele jako takové, může zaměstnavateli kvůli tomu hrozit i vysoké reputační riziko a s tím spojená ztráta důvěry zákazníků. To vše může v krajním případě vyústit v ukončení činnosti zaměstnavatele, tedy zánik pracovních míst; v tomto kontextu proto může být monitoring aktivit zaměstnanců také paradoxně též v jejich zájmu. Specifickým případem jsou pak zaměstnavatelé, kterým povinnost chránit informace a zachovávat mlčenlivost ukládají obecně závazné právní předpisy (např. banky, advokáti, daňoví poradci, auditoři, insolvenční správci, atd.). Pro tyto zaměstnavatele je nesmírně důležité hlídat aktivitu zaměstnanců a bránit tak možnému porušení právních předpisů a z toho vyplývajícím negativním důsledkům.

Každý zaměstnavatel si také pochopitelně přeje, aby jeho zaměstnanci pracovali co nejvíce a co nejefektivněji. Nelze tedy zaměstnavatelům vyčítat, že si přejí mít pod kontrolou činnost svých zaměstnanců a bránit zneužívání pracovních prostředků pro soukromé účely. Ostatně podle § 301 písm. b) ZP jsou zaměstnanci povinni využívat pracovní dobu a výrobní prostředky k vykonávání svěřených prací a podle téhož paragrafu, písm. d), mají povinnost řádně hospodařit s prostředky svěřenými jim zaměstnavatelem a střežit a ochraňovat majetek zaměstnavatele před poškozením, ztrátou, zničením a zneužitím a nejednat v rozporu s oprávněnými zájmy zaměstnavatele. Také Evropský soud pro lidská práva konstatoval, že od zaměstnavatelů je třeba rozumně očekávat potřebu ověřovat si, že se jejich zaměstnanci během pracovní doby skutečně věnují pracovním úkolům, a to i v případech, kdy zaměstnanci svým jednáním nezpůsobují zaměstnavateli žádnou skutečnou újmu (nepočítaje v to pochopitelně újmu odpovídající mzdě poskytované zaměstnavatelem zaměstnanci za čas strávený soukromými aktivitami).[18]

Lze říci, že zavedení kontrolních mechanismů má funkci preventivní a represivní. Vědí-li zaměstnanci, že jejich aktivity v práci jsou ze strany zaměstnavatele

[18] Rozsudek Evropského soudu pro lidská práva, stížnost č. 61496/08, ze dne 12. ledna 2016, Věc Bărbulescu proti Rumunsku.

zaznamenávány a vyhodnocovány, budou se zpravidla snažit své nepracovní a případné jiné nežádoucí činnosti omezit (nebo sledovací opatření obejít). Funkci represivní pak představuje možnost zaměstnavatele vyvodit z aktivity zaměstnanců důsledky, např. v podobě rozvázání pracovního poměru, vymáhání náhrady škody a v krajním případě i podání trestního oznámení.

V případě zaměstnavatelů – právnických osob pak do hry vstupuje další faktor, a to povinnost jejich statutárních (případně i dozorčích) orgánů vykonávat svou funkci s péčí řádného hospodáře. Každý člen statutárního orgánu tak v konečném důsledku v plném rozsahu odpovídá za ochranu majetku společnosti i za to, že zaměstnanci řádně a efektivně pracují a že jsou v právnické osobě nastaveny vhodné mechanismy, které tyto cíle pomáhají sledovat. Jedním z těchto mechanismů může být právě zavedení monitoringu zaměstnanců.

1.3 Princip proporcionality

Ústavně zaručené právo zaměstnanců na soukromí pochopitelně naráží na ústavně zaručené právo zaměstnavatele na ochranu majetku. V případě takového konfliktu dvou základních práv, která jsou si vzájemně rovna, je třeba provést jejich poměření při užití principu proporcionality za současného šetření podstaty a smyslu obou základních práv, jak požaduje čl. 4 odst. 4 Listiny základních práv a svobod. Přitom je však dle judikatury Ústavního soudu třeba dbát, aby bylo dosaženo co nejširšího uplatnění obou chráněných hodnot.[19]

Vzájemné poměřování ústavně zaručených práv spočívá v provedení testu proporcionality, který je nutné provést před upřednostněním jednoho takového práva před druhým. Podle Ústavního soudu spočívá tento test v postupném vyhodnocení následujících kritérií: (i) kritérium vhodnosti, tj. lze-li pomocí prostředku (monitoringu zaměstnanců) omezujícího určité základní právo (právo zaměstnanců na ochranu soukromí) dosáhnout sledovaný cíl (ochranu práva zaměstnavatele na majetek); (ii) kritérium potřebnosti, tj. zda je daný prostředek, který omezuje základní právo, skutečně nezbytný pro dosažení sledovaného cíle, nebo zda lze tohoto cíle dosáhnout

[19] Nález Ústavního soudu sp. zn. I. ÚS 321/06 ze dne 18. prosince 2006.

i jinými prostředky, které do základního práva v kolizi nezasahují; a (iii) porovnání závažnosti obou v kolizi stojících základních práv (po kladném vyhodnocení obou předchozích kritérií), jež spočívá ve zvažování a) empirických argumentů (tj. faktické závažnosti jevu, který je spojen s ochranou určitého základního práva), b) systémových argumentů (tj. zvažování smyslu a zařazení dotčeného základního práva či svobody v systému základních práv a svobod), c) kontextových argumentů (tj. dalších negativních dopadů omezení jednoho základního práva v důsledku upřednostnění jiného) a d) hodnotových argumentů (tj. zvažování pozitiv v kolizi stojících základních práv vzhledem k akceptované hierarchii hodnot).[20] Třetí z výše jmenovaných kritérií bude ve prospěch omezení práva zaměstnanců na soukromí splněno tehdy, pokud lze důvodně očekávat, že užitek zaměstnavatele dosažený pomocí monitoringu zaměstnanců bude vyšší než nepříznivé dopady monitoringu na soukromí zaměstnanců.[21] Tuto zásadu vyjadřuje i GDPR, když v čl. 6 odst. 1 písm. f) uvádí, že zpracování osobních údajů za účelem ochrany práv a právem chráněných zájmů správce nebo jiných dotčených osob lze provádět s výjimkou případů, kdy před takovými zájmy zaměstnavatele mají přednost zájmy nebo základní práva a svobody zaměstnanců vyžadující ochranu osobních údajů. Obdobně též ZOOÚ stanoví, že zpracování osobních údajů za účelem ochrany práv a právem chráněných zájmů správce nebo jiných dotčených osob nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života (§ 5 odst. 2 písm. e) ZOOÚ).

Dle stanoviska ÚOOÚ ohledně ochrany soukromí zaměstnanců se zřetelem k monitoringu pracoviště je zásada proporcionality první vůdčí zásadou, kterou je zaměstnavatel povinen při zavádění sledovacích opatření aplikovat. Oprávnění zaměstnance musejí být dle ÚOOÚ na základě principu proporcionality v rovnováze s legitimními oprávněními a zájmy zaměstnavatele, což vychází z rozložení práv a povinností zaměstnance a zaměstnavatele v rámci pracovněprávního vztahu. Zaměstnanec totiž může legitimně očekávat, že i na pracovišti bude ze strany zaměstnavatele přiměřeně zachováváno jeho právo na soukromí; zároveň má však zaměstnavatel právo vyžadovat ze strany zaměstnanců efektivní práci, chránit svou

[20] Nález Ústavního soudu sp. zn. Pl. ÚS 4/94 ze dne 12. října 1994.

[21] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, dostupné elektronicky v systému ASPI, Část I., kapitola 3.5. ISBN 978-80-7478-139-1.

činnost před nežádoucím jednáním zaměstnanců a také požadovat, aby zaměstnanci své soukromé záležitosti vyřizovali v pracovní době pouze v přiměřené a nezbytné míře.[22]

Jak uvádí Pracovní skupina též s ohledem na znění GDPR, je zaměstnavatel, který zpracovává osobní údaje zaměstnanců za účelem ochrany svých práv a právem chráněných zájmů, povinen přijmout taková opatření, která zajišťují vzájemnou rovnováhu oprávněných zájmů zaměstnavatele a základních práv a svobod zaměstnance a zaručují, že zásah do práva zaměstnance na soukromí bude co nejmenší. V případě monitoringu zaměstnanců se může dle Pracovní skupiny jednat kupříkladu o (i) geografická opatření (např. kamerový systém zacílený pouze na určitá místa, kde hrozí nejvyšší nebezpečí pro zájmy zaměstnavatele; snímání prostorů toalet a odpočíváren by přitom mělo být obecně zakázáno), (ii) opatření zamířená na minimalizaci sledovaných dat (např. vynětí soukromých složek uložených na počítači nebo soukromé komunikace z monitoringu), a (iii) časová opatření (např. časově omezený monitoring namísto dlouhotrvajícího monitoringu).[23]

Jak vyplývá z výše uvedeného výkladu, jsou zaměstnavatelé povinni velmi pečlivě zvažovat, jak monitoring provádět a jaká opatření v jeho rámci přijmout, aby byly jejich zájmy dostatečně chráněny a zároveň aby docházelo k co nejmenším zásahům do soukromí zaměstnanců. Správné vyhodnocení situace je klíčem k legitimnímu sledování zaměstnanců.

1.4 Oprávnění zaměstnavatele monitorovat zaměstnance

Z principu proporcionality vycházel zákonodárce, když prostřednictvím ZP obecně určil podmínky, za nichž lze omezit právo zaměstnanců na soukromí ve prospěch práva zaměstnavatele na ochranu majetku.

Dle § 316 odst. 1 ZP platí, že zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní

[22] ÚOOÚ: Stanovisko č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. Únor 2009.

[23] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 7 – 8.

techniky ani jeho telekomunikační zařízení; dodržování tohoto zákazu je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat. Tento zákaz je absolutní a je vyjádřením práva zaměstnavatele jako vlastníka těchto prostředků určit, jak bude s jeho majetkem zacházeno. Pokud zaměstnavatel zaměstnancům užívání výrobních a pracovních prostředků pro osobní potřebu nedovolí, nejsou zaměstnanci nijak oprávněni je takto užívat, a to dokonce ani ve svém volném čase mimo pracovní dobu nebo v případě, že jim zrovna zaměstnavatel v pracovní době nepřiděluje žádnou práci.[24] Povolení k soukromému užívání těchto prostředků zaměstnavatel zaměstnancům uděluje zpravidla přímo v pracovní smlouvě nebo, flexibilněji ve svůj prospěch, ve vnitřním předpisu. Lze zaměstnavateli doporučit, aby rovněž stanovil podrobnější a jasná pravidla pro takové soukromé užívání (např. omezení užívání na určitý počet hodin v měsíci během pracovní doby a/nebo na období mimo pracovní dobu, omezení výše provolané částky, omezení přístupu na určité internetové stránky, apod.).

Co se týče otázky přiměřeného způsobu kontroly zákazu užívání výrobních prostředků zaměstnavatele pro soukromé účely, nabídl určitá vodítka ve své rozhodovací praxi Nejvyšší soud. Dle něj je třeba vzít při hodnocení přiměřenosti kontroly v úvahu zejména skutečnost, zda se jedná o kontrolu průběžnou či následnou, jak dlouho trvá, v jakém rozsahu je prováděna, zda vůbec a do jaké míry omezovala zaměstnance v jeho činnosti a zasahovala do jeho práva na soukromí, atd. Předmětem kontroly smí být pouze zjištění, zda zaměstnanec zákaz porušil.[25] Zaměstnavatel tudíž není oprávněn sledovat ani zaznamenávat obsah soukromého jednání zaměstnance (např. soukromou komunikaci doručenou do soukromé e-mailové schránky, soukromé hovory, SMS zprávy, obsah prohlížených internetových stránek, apod.). V tomto smyslu Nejvyšší soud jako přiměřený způsob kontroly ve své rozhodovací praxi podpořil (i) skryté sledování aktivity zaměstnance na internetu po dobu jednoho měsíce[26], což je dle mého názoru poměrně kontroverzní (viz podrobněji výklad v kapitole 1.5.2(b) níže),

---

[24] Viz např. MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, dostupné elektronicky v systému ASPI. Část I., kapitola 2.1.1. ISBN 978-80-7478-139-1. Argument, že užívání internetového připojení bez dovolení zaměstnavatele je v pořádku za situace, kdy zaměstnavatel nepřiděluje zaměstnanci práci, použil neúspěšně zaměstnanec jako žalobce ve sporu definitivně rozhodnutém Nejvyšším soudem dne 7. srpna 2014, vedeném pod sp. zn. 21 Cdo 747/2013 (tento případ je detailně rozebrán v kapitole 2.2.4(b)).

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

[26] Tamtéž.

a (ii) pořízení výpisu hovorů zaměstnance za období jednoho měsíce, učiněných z mobilního telefonu přiděleného zaměstnavatelem.[27]

Relevantní je v tomto směru též poměrně nedávný rozsudek Evropského soudu pro lidská práva ve věci Bărbulescu proti Rumunsku. V něm soud připustil, že zaměstnavatel byl oprávněn zkontrolovat komunikaci zaměstnance učiněnou prostřednictvím aplikace Yahoo! Messenger, kterou byl zaměstnanec oprávněn používat pouze pro pracovní účely. Z kontroly trvající po dobu 9 dnů vyplynulo, že zaměstnanec tuto aplikaci používal též pro soukromé účely, a zaměstnavatel s ním proto rozvázal pracovní poměr pro porušování jím stanovených povinností. Soud konstatoval, že přestože zaměstnavatel použil proti zaměstnanci jako důkaz podrobný výpis zpráv, které si zaměstnanec pomocí této aplikace se svým bratrem a snoubenkou vyměnil (a které obsahovaly kromě jiného též informace intimního charakteru a údaje o zdravotním stavu zaměstnance), neporušil právo zaměstnance na soukromí garantované čl. 8 Úmluvy o ochraně lidských práv a základních svobod, neboť pracovní poměr s ním rozvázal nikoli na základě zjištěného obsahu soukromých zpráv, ale pouze z důvodu, že zaměstnanec porušil zákaz neužívat pracovní prostředky zaměstnance pro jiné než pracovní účely.[28]

Monitoring zaměstnanců v užším slova smyslu však vychází až z § 316 odst. 2 ZP. Dle tohoto ustanovení nesmí zaměstnavatel bez závažného důvodu spočívajícího ve zvláštní povaze své činnosti narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že by zaměstnance podroboval otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci. Jestliže je však u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze jeho činnosti, který odůvodňuje zavedení kontrolních mechanismů, je zaměstnavatel oprávněn své zaměstnance monitorovat. Ustanovení § 316 odst. 3 ZP zaměstnavateli pak ukládá, aby v takovém případě své zaměstnance přímo informoval o rozsahu kontroly a způsobech jejího provádění.

---

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

[28] Rozsudek Evropského soudu pro lidská práva, stížnost č. 61496/08, ze dne 12. ledna 2016, Věc Bărbulescu proti Rumunsku.

Zákoník práce ovšem ani příkladmo nedefinuje, jaký závažný důvod by zaměstnavatel měl mít, respektive jakou zvláštní činnost by měl vykonávat, aby byl oprávněn monitoring zaměstnanců zavést. Konkrétní v tomto ohledu není ani důvodová zpráva k návrhu na vydání zákoníku práce, která se v komentáři k ustanovení § 316 ZP pouze omezila na konstatování, že v dosavadní právní úpravě chyběla úprava řešení ochrany majetkových zájmů zaměstnavatele a také ochrana osobních práv zaměstnance v pracovněprávních vztazích.[29] Zákon č. 65/1965 Sb., zákoník práce, ve znění pozdějších předpisů, účinný do 31. prosince 2006, skutečně úpravu podmínek sledování zaměstnanců neobsahoval. Výklad pojmu zvláštní činnosti tak musejí v konečném sledu zaujmout soudy; to však nebrání i jiným institucím vyjádřit svůj názor na tuto problematiku.

Státní úřad inspekce práce míval, vcelku pochopitelně s ohledem na své poslání - ochranu zaměstnanců proti zaměstnavatelům, tendenci chápat pojem zvláštní činnosti zaměstnavatele velice úzce. Přesto s odstupem času „polevil“ ve prospěch zaměstnavatelů. Ve svých manuálech ze srpna 2010 a ledna 2011 totiž přiznával povahu zvláštní činnosti pouze zaměstnavatelům typu vězeňské služby, pokladny čerpací stanice, banky, policejní služebny apod. Zároveň odmítal výklad, že by pod pojem závažného důvodu spočívajícího ve zvláštní činnosti zaměstnavatele mohla spadat např. též ochrana majetku zaměstnavatele a zdraví a bezpečnosti zaměstnanců, kontrola dodržování technologie či prevence.[30] Ve svém nejnovějším manuálu z května 2014 se však Státní úřad inspekce práce omezuje pouze na konstatování, že z jeho pohledu zpravidla není závažný důvod dán při výrobě běžných výrobků nebo při poskytování běžných služeb s tím, že hodnocení je vždy třeba vztáhnout ke konkrétnímu pracovišti a konkrétnímu zaměstnavateli.[31] Takový výklad je sice poměrně vágní (je otázkou, co vše lze ještě z pohledu orgánů inspekce práce chápat jako „běžné výrobky a služby“),

---

[29] Vládní návrh na vydání zákoníku práce, sněmovní tisk 1153, s. 271, dostupný též z WWW: <http://www.psp.cz/sqw/text/tiskt.sqw?O=4&CT=1153&CT1=0>.

[30] Viz (i) Státní úřad inspekce práce, odbor pracovních vztahů a podmínek: Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele. Srpen 2010; a (ii) Státní úřad inspekce práce, odbor pracovních vztahů a podmínek: Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele. Leden 2011.

[31] Státní úřad inspekce práce, odbor pracovních vztahů a podmínek: Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele. Květen 2014.

ale oproti těm původním přesto dává zaměstnavateli relativně širokou možnost argumentovat ve prospěch zavedení sledovacích opatření.

Poměrně restriktivní výklad pojmu zvláštní činnosti zaměstnavatele nicméně zastává ÚOOÚ. Ve svém stanovisku k této problematice a v související rozhodovací praxi dlouhodobě uvádí, že za takovou činnost lze považovat např. mezinárodní bankovní převody nebo dozor nad prací vězňů[32], popřípadě provozy, v nichž se pracuje s vysoce nebezpečnými chemikáliemi (a zavedený kamerový systém pomáhá kontrolovat dodržení pracovního postupu při práci s těmito chemikáliemi, kdy jsou zaměstnanci dennodenně vystaveni vysokému riziku ohrožení života a zdraví, přičemž vyhodnocování kamerových záznamů může pomoci zjistit např. to, která činnost představuje největší riziko, díky čemuž mohou být pracovní postupy upraveny tak, aby byla rizikovost práce minimalizována) nebo v nichž se nakládá s vysokými finančními částkami (kdy např. zavedený kamerový systém slouží k ochraně zaměstnanců, neboť zde existuje poměrně velké riziko přepadení).[33] Za zvláštní povahu činnosti tak ve svých rozhodnutích neuznal např. doručování poštovních zásilek ze strany České pošty, s.p., byť současně konstatoval, že jde o zajišťování veřejného zájmu společnosti[34] (bližší rozbor tohoto rozhodnutí viz v kapitole 2.4.4 níže), ani běžné provozování autobusové přepravy ze strany STUDENT AGENCY, k.s. (bližší rozbor tohoto rozhodnutí viz v kapitole 2.3.4(b) níže).[35] Tyto výklady ÚOOÚ podpořil též Městský soud v Praze v řízeních o správních žalobách, které oba uvedení zaměstnavatelé podali. V rozsudku týkajícím se společnosti STUDENT AGENCY, k.s., soud konstatoval, že o zvláštní povaze provozu autobusové dopravy nelze hovořit, neboť se nejedná ve své podstatě o činnost nebezpečnou[36], a v argumentaci se tak přiklonil k velmi restriktivnímu chápání pojmu zvláštní činnosti zaměstnavatele. V později vydaném rozsudku týkajícím se České pošty, s.p., soud nicméně argumentoval poněkud odlišně; povahu činnosti zaměstnavatele neshledal natolik zvláštní, aby mohla v daném případě

---

[32] ÚOOÚ: Stanovisko č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště, s. 4. Únor 2009.

[33] Rozhodnutí předsedy Úřadu pro ochranu osobních údajů, č. j. UOOU-00363/13-41 ze dne 24. dubna 2013.

[34] Rozhodnutí Úřadu pro ochranu osobních údajů, č. j. UOOU-00237/13-38 ze dne 3. července 2013.

[35] Rozhodnutí předsedy Úřadu pro ochranu osobních údajů, č. j. UOOU-00363/13-41 ze dne 24. dubna 2013.

[36] Rozsudek Městského soudu v Praze sp. zn. 5 A 107/2013 ze dne 18. října 2016.

odůvodnit zavedení příslušného kontrolního mechanismu, který podstatně narušoval soukromí zaměstnanců, tj. aplikoval test proporcionality a vyhodnotil, že za konkrétně daných okolností nebyl splněn.[37] Ve druhém zmíněném případě tak soud dle mého názoru připustil širší chápání pojmu zvláštní činnosti zaměstnavatele, a to v závislosti na míře zásahu použitého prostředku monitoringu do soukromí zaměstnavatele. Oba případy rozhodovaly vesměs odlišně složené správní senáty[38]; je proto otázkou, zda se k těmto případům bude vyjadřovat Nejvyšší správní soud a jaké stanovisko zaujme. Společnost STUDENT AGENCY, k.s., proti rozhodnutí Městského soudu v Praze podala kasační stížnost a řízení u Nejvyššího správního soudu je vedeno pod sp. zn. 10 As 245/2016; ke dni odevzdání této práce však případ nebyl rozhodnut. Česká pošta, s.p., kasační stížnost nepodala. Prozatím se bohužel k otázce pojmu zvláštní činnosti zaměstnavatele žádný soud nejvyššího stupně, potažmo Ústavní soud, nevyjádřil.

Výklady v odborné literatuře přiznávají právo monitorovat své zaměstnance za splnění určitých podmínek v podstatě každému zaměstnavateli.[39] Vycházejí zejména ze stanoviska č. 8/2001 o zpracování osobních údajů v kontextu zaměstnání vydaného Pracovní skupinou. Z tohoto stanoviska vyplývá, že zaměstnavatel je oprávněn monitorovat své zaměstnance za předpokladu, že je takový monitoring přiměřenou reakcí zaměstnavatele na rizika, kterým čelí, se zohledněním legitimních zájmů sledovaných zaměstnanců, co se týče jejich soukromí. Rozsah osobních údajů, s nimiž zaměstnavatel v průběhu monitoringu nakládá, musí být s ohledem na daný ospravedlnitelný účel přiměřený a relevantní a nesmí být excesivní. Veškerý monitoring musí být prováděn tak, aby co nejméně zasahoval do práv zaměstnanců, a musí být cílený na rizika, kvůli nimž byl zaveden (rozbor těchto i dalších zásad monitoringu viz v kapitole 1.5.2 níže).[40] Bohužel ani toto stanovisko neuvádí žádné konkrétní příklady oprávněného či excesivního monitoringu co se týče důvodu jeho zavedení. Omezuje se pouze na konstatování, že na takovou otázku neexistuje definitivní odpověď a že míra

[37] Rozsudek Městského soudu v Praze sp. zn. 6 A 42/2013 ze dne 5. května 2017.

[38] Pouze jedna ze tří soudkyň zasedala v obou z těchto senátů.

[39] BĚLINA, Miroslav a kolektiv. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015, xviii, s. 1242. Velké komentáře. ISBN 978-80-7400-290-8.

[40] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 8/2001 o zpracování osobních údajů v kontextu zaměstnání (v originále: „*Opinion 8/2001 on the processing of personal data in the employment context*“) ze dne 13. září 2001, s. 25.

tolerovatelného zásahu do soukromí zaměstnanců vždy záleží na povaze zaměstnání a souvisejících specifických okolnostech, tj. že bude nepochybně na jiné úrovni v případě bezpečnostního technika zaměstnaného u Evropské centrální banky než u zaměstnance kavárny pracujícího v té samé budově.[41] Nové postřehy v tomto směru nepřineslo ani nedávné stanovisko Pracovní skupiny č. 2/2017, které bylo vydáno především s ohledem na GDPR i na dostupnost nových technologií, jež od roku 2001 pochopitelně zaznamenaly rapidní rozvoj.[42]

Ani dle mého názoru nelze omezit možnost monitorovat zaměstnance pouze na zaměstnavatele vykonávající zvláště nebezpečnou činnost. Přikláním se k závěru, že za splnění principu proporcionality a dodržení zásad, které jsou pro monitoring a související ochranu soukromí zaměstnanců klíčové (viz zejména kapitolu 1.5.2 níže), může zaměstnance monitorovat prakticky každý zaměstnavatel. Např. se domnívám, že za zvláštní povahu činnosti zaměstnavatele ospravedlňující monitoring elektronické pošty zaměstnanců lze považovat situaci, kdy hlavní (podnikatelskou) činnost zaměstnavatele vykonávají tito zaměstnanci v zásadě nepřetržitou prací na počítači. Závažným důvodem k zavedení monitoringu zaměstnanců spočívajícím ve zvláštní povaze činnosti zaměstnavatele pak může být typicky např. ochrana majetku zaměstnavatele, ochrana bezpečnosti a zdraví zaměstnanců, síťová bezpečnost, ochrana utajovaných skutečností, bankovního nebo obchodního tajemství, důvěrných informací nebo know-how, kontrola dodržování povinnosti mlčenlivosti ze strany zaměstnanců, apod.

V odborné literatuře se lze dále setkat se dvěma přístupy k výkladu podmínek, jež ustanovení § 316 odst. 2 ZP zaměstnavatelům stanoví. František Nonnemann dochází k závěru, že pouze zvláštní povaha činnosti zaměstnavatele jej sama o sobě neopravňuje sledovat své zaměstnance; k zavedení kontrolních mechanismů musí mít zaměstnavatel rovněž objektivně závažný důvod vycházející právě ze zvláštní povahy činnosti zaměstnavatele. Nonnemann tudíž spatřuje ve znění § 316 odst. 2 ZP dvě podmínky,

---

41 Tamtéž, s. 19.

42 Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017.

které musí zaměstnavatel splnit současně.[43] Naproti tomu podle Jakuba Morávka není takový výklad s ohledem na aplikační praxi vhodný, mimo jiné i proto, že trvání na kumulativním splnění obou podmínek by vedlo k dalšímu zúžení případů, kdy by byl monitoring zaměstnanců oprávněný.[44] K tomuto závěru se přikláním též. Dle mého názoru nelze vykládat pojem „závažný důvod" mimo rámec zvláštní povahy činnosti zaměstnavatele; právě tato zvláštní povaha činnosti zaměstnavatele je základem pro existenci zvláštního důvodu, který ospravedlňuje zavedení monitoringu zaměstnanců.

Převažuje názor, že § 316 odst. 2 ZP se uplatní pouze na zaměstnavatele, kteří mají v úmyslu zavést zvlášť intenzivní, systematické a dlouhodobé sledování zaměstnanců.[45] Ačkoli takový závěr neplyne ani z důvodové zprávy, ani z judikatury, Nonnemann jej dovozuje z terminologie, kterou zákonodárce v tomto ustanovení použil; pojmy jako sledování, odposlech či záznam jsou podle něj z podstaty věci spojeny s delší než jednorázovou aktivitou. Rovněž pojem „kontrola" elektronické či písemné pošty podle něj spíše představuje pravidelnou aktivitu, a nikoli pouze jednorázový jev.[46] K témuž závěru dochází v kontextu monitoringu zaměstnanců pomocí GPS technologie Zuzana Radičová.[47]

Pokud tedy zaměstnavatel provede jednorázovou či nahodilou kontrolu zaměstnance (např. zda neužívá jemu svěřené pracovní prostředky pro soukromé účely bez souhlasu zaměstnavatele ve smyslu § 316 odst. 1 ZP), je oprávněn tak učinit i přesto, že k tomu nemá závažný důvod spočívající ve zvláštní povaze jeho činnosti. Takový závěr je ostatně rozumný právě s ohledem na ustanovení § 316 odst. 1 ZP; proč by měla být možnost kontroly dodržování zde stanoveného zákazu omezena na zaměstnavatele, kteří současně splňují podmínku dle odst. 2 téhož ustanovení. Opačný výklad by byl dle

---

43 NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 232. ISSN 1210-6410.

44 MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, dostupné elektronicky v systému ASPI. Část V., kapitola 2.1.1. ISBN 978-80-7478-139-1.

45 Např. BĚLINA, Miroslav a kolektiv. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015, xviii, s. 1242. Velké komentáře. ISBN 978-80-7400-290-8, a autoři citovaní pod body 46 a 47 níže.

46 NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 232. ISSN 1210-6410.

47 RADIČOVÁ, Zuzana. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy*. 2014, roč. 22, č. 21, s. 737. ISSN 1210-6410.

mého názoru v rozporu s ústavně zaručeným právem zaměstnavatele na ochranu majetku.

Uveďme nicméně i další typy nahodilého sledování zaměstnanců, které nebudou vůbec spadat pod § 316 ZP. Půjde např. o snímání vstupu do areálu zaměstnavatele kamerovým systémem, který má sloužit k ochraně prostor před vstupem nepovolaných osob (a chtě nechtě zachytí i zaměstnance při příchodu a odchodu do/z práce), nebo o nahodilý *mystery shopping*, tj. situaci, kdy je zaměstnancovo vystupování vůči zákazníkům nahodile testováno osobou pověřenou zaměstnavatelem, která vůči zaměstnanci vystupuje jako běžný zákazník.[48] Zaměstnavatel pak vyhodnocuje jednání zaměstnance, zpravidla na základě jednorázové audio či videonahrávky nebo e-mailové komunikace.[49]

1.5 Parametry provádění monitoringu

Zaměstnavatel by měl před zavedením příslušného kontrolního mechanismu vždy zvážit, zda je důvod pro jeho používání závažný natolik, aby byl monitoring zaměstnanců ospravedlnitelný a přiměřený, a měl by se zasadit o to, aby nedocházelo k nepřiměřenému zásahu do soukromí zaměstnanců. Zároveň by měl zaměstnavatel předem uvážit, zda v daném konkrétním případě neexistuje jiný způsob, jakým by bylo možné dosáhnout potřebného účelu, tedy ochrany jeho majetkových práv. Pokud by taková cesta existovala, byť by byla pro zaměstnavatele technicky či administrativně složitější, pak by s ohledem na test proporcionality mohla být oprávněnost zavedení kontrolních mechanismů a sledování zaměstnanců zpochybněna. Tento princip nyní výslovně obsahuje i GDPR; v recitálu 39 stanoví, že osobní údaje by měly být zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky.

V každém případě monitoring zaměstnanců podléhá určitým zásadám, které si rozebereme v této kapitole. Nejprve je však potřeba zodpovědět otázku, kdy monitoring

[48] DURUGY, Andras, KOLLAR, Peter. On the Use of Mystery Shopping to Measure Competences. *Journal of Human Resource Management*. 2017, roč. XX, č. 1, s. 81. ISSN 2453-7683.

[49] NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 234. ISSN 1210-6410.

zaměstnanců zároveň představuje zpracování osobních údajů, tj. kdy se na něj uplatní také ZOOÚ a GDPR, jakmile nabyde účinnosti. Připomeňme v této souvislosti též Kodex ochrany osobních údajů zaměstnanců, který vydala Mezinárodní organizace práce. Ten sice představuje pouze soubor nezávazných zásad a doporučení, ale v rámci dobré praxe by jej měli zaměstnavatelé (a rovněž zákonodárci při tvorbě právních předpisů) brát v úvahu.[50] Vesměs však obsahuje zásady, které již upravuje ZOOÚ a GDPR, s tím, že nakládání s osobními údaji zaměstnanců (včetně monitoringu) má být prováděno tak, aby byla zaručena důstojnost zaměstnanců, ochrana jejich soukromí a zaručeno jejich základní právo na určení, kdo může používat jejich osobní údaje, za jakým účelem a za jakých podmínek (čl. 1 – preambule). Dalším mezinárodním dokumentem v oblasti ochrany osobních údajů, který je ovšem na rozdíl od zmíněného Kodexu právně závazný, je Úmluva č. 108 o ochraně osob s ohledem na automatizované zpracování osobních dat ze dne 28. ledna 1981, přijatá na půdě Rady Evropy; pro Českou republiku vstoupila v platnost dne 1. listopadu 2001. Její ustanovení jsou však vesměs promítnuta již v ZOOÚ i GDPR.

1.5.1 Kdy monitoring zaměstnanců představuje zpracování osobních údajů

V souladu s § 4 písm. e) ZOOÚ rozumíme zpracováním osobních údajů jakoukoliv operaci nebo soustavu operací, které správce nebo zpracovatel[51] systematicky provádějí s osobními údaji[52], a to automatizovaně nebo jinými prostředky. Totéž ustanovení pak

---

[50] MEZINÁRODNÍ ORGANIZACE PRÁCE: *Kodex ochrany osobních údajů zaměstnanců* (v originále: „*Protection of Worker's Personal Data*"). 1. vydání. Ženeva: International Labour Office, 1997, 24 s. ISBN 92-2-110329-3.

[51] Správcem osobních údajů bude v našem případě zaměstnavatel; dle § 4 písm. j) ZOOÚ určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Pokud zaměstnavatel pověří vlastním zpracováváním osobních údajů třetí subjekt, bude tento zpracovatelem ve smyslu § 4 písm. k) ZOOÚ.

[52] Připomeňme legální definici osobních údajů a jejich podmnožiny, citlivých údajů. Dle § 4 písm. a) ZOOÚ je osobním údajem „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*." Dle § 4 písm. b) ZOOÚ je pak citlivým údajem „*osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů*." Subjektem údajů je v našem případě zaměstnanec. GDPR vesměs obsahuje obdobnou definici osobních údajů v čl. 4 odst. 1; výslovně jako osobní údaj nicméně zmiňuje síťový identifikátor (typicky půjde o soubory cookies), lokační údaje a genetickou identitu

obsahuje demonstrativní výčet operací, které představují zpracování osobních údajů: jejich shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.[53] Za významný prvek této definice je třeba považovat pojem „systematičnosti" nakládání s osobními údaji; dle eurokonformního výkladu je nicméně nutné chápat veškeré automatizované či částečně automatizované zpracování osobních údajů za systematické a pouze u manuálních způsobů nakládání s osobními údaji lze případně uvažovat o absenci tohoto prvku.[54] Sledování zaměstnanců přitom zpravidla probíhá právě pomocí (částečně) automatizovaných prostředků, tj. systematicky.

Ve většině případů (včetně nahodilého sledování zaměstnanců, které nespadá pod úpravu § 316 ZP) dochází k takovému nakládání s osobními údaji zaměstnanců, že lze mluvit o jejich zpracovávání ve smyslu výše uvedené definice. Ovšem v situacích, kdy ke sběru osobních údajů ve smyslu ZOOÚ nedochází, např. při živém odposlechu telefonních hovorů zaměstnanců nebo při snímání zaměstnanců kamerovým systémem bez záznamu, o zpracování osobních údajů nepůjde, a ZOOÚ, potažmo GDPR, se tudíž neuplatní.[55] O zpracování osobních údajů se např. nebude jednat ani v případě, kdy zaměstnavatel jednorázově nahlédne do elektronické pošty zaměstnance, který je dlouhodoběji nepřítomen na pracovišti, z důvodu nezbytného vyřízení pracovní komunikace doručené pouze tomuto zaměstnanci[56].

V pracovněprávních vztazích nelze uvažovat o výjimce stanovené v § 3 ZOOÚ, podle níž se ZOOÚ nevztahuje na zpracování osobních údajů, které provádí fyzická osoba

---

subjektu údajů. Citlivé údaje označuje GDPR jako zvláštní kategorie osobních údajů; jejich definici, která je obdobná stávající definici dle ZOOÚ, uvádí v čl. 9 odst. 1.

53 Obdobnou definici zpracování osobních údajů obsahuje též čl. 4 odst. 2 GDPR; jako příklad zpracování dále ještě uvádí „strukturování", „přizpůsobení" a „nahlédnutí".

54 KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel: *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck, 2012, s. 68 – 69. ISBN 978-80-7179-226-0.

55 BĚLINA, Miroslav a kolektiv. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015, xviii, s. 1243. Velké komentáře. ISBN 978-80-7400-290-8; NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 233. ISSN 1210-6410.

56 ÚOOÚ: K problémům z praxe, č. 1/2013 – Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců [online]. [cit. 4. listopadu 2017] Dostupné z WWW: <https://www.uoou.cz/c-1-2003-monitorovani-elektronicke-posty-a-ochrana-soukromi-a-osobnich-udaju-zamestnancu/ds-2551/archiv=0&p1=2551>.

výlučně pro osobní potřebu. I přesto, že by byl zaměstnavatel fyzickou osobou, nebylo by možné pokládat monitoring zaměstnanců jako vykonávaný pro jeho osobní potřebu; zaměstnavatel jej totiž využívá v rámci své podnikatelské činnosti, která již z povahy věci nepředstavuje jeho osobní potřebu.[57] Pojem zpracování pro osobní potřebu je totiž třeba chápat pouze jako takové, jež fyzická osoba provádí pro naplnění vlastních subjektivních potřeb, konkrétně za účelem realizace svého běžného soukromého a osobního života, a to zejména ve smyslu možnosti styku s jinými lidmi (samozřejmě za předpokladu, že takové zpracování nenaráží na práva ostatních osob).[58] V tomto směru chápe „osobní potřebu" také GDPR, když v recitálu 18 uvádí, že činnosti čistě osobní povahy (a činnosti prováděné výhradně v domácnosti)[59] jsou činnostmi bez jakékoli souvislosti s profesní nebo obchodní činností. Takto výslovné vyloučení „osobní potřeby" v rámci podnikatelské činnosti Směrnice 95/46/ES neobsahovala.[60]

1.5.2 Zásady monitoringu a povinnosti zaměstnavatele

Aby byl monitoring zaměstnanců oprávněný, musí splňovat řadu kritérií, která stanoví na jedné straně ZP a na druhé ZOOÚ/GDPR (tyto se použijí s výjimkou případů, kdy monitoring zaměstnanců nepředstavuje zpracování osobních údajů – viz předchozí kapitola). Zásady zpracování osobních údajů zaměstnanců vypočítává též Pracovní skupina ve stanovisku č. 8/2001[61] ve spojení se stanoviskem č. 2/2017.[62] V souvislosti s naplňováním jednotlivých zásad je na zaměstnavatele kladena řada povinností, jejichž okruh se ještě rozšíří s účinností GDPR.

---

[57] Viz např. MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, dostupné elektronicky v systému ASPI. Část IV., kapitola 2, komentář k § 3. ISBN 978-80-7478-139-1.

[58] MORÁVEK, Jakub. Osobní potřeba – neurčitý právní pojem? *Právní rozhledy*. 2010, roč. 18, č. 24, s. 871 – 872. ISSN 1210-6410.

[59] Pro úplnost, GDPR za činnost osobní povahy příkladmo v tomtéž článku uvádí korespondenci a vedení adresářů nebo využívání sociálních sítí a internetu v souvislosti s těmito činnostmi.

[60] Směrnice 95/46/ES v recitálu 12 pouze uváděla, že „*je třeba vyloučit zpracování údajů fyzickou osobou při výkonu činností, které mají výlučně osobní povahu, jako je korespondence nebo vedení adresáře*".

[61] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 8/2001 o zpracování osobních údajů v kontextu zaměstnání ze dne 13. září 2001 (v originále: „*Opinion 8/2001 on the processing of personal data in the employment context*"), s. 20 – 22 a 24 – 25.

[62] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*") ze dne 8. června 2017.

(a) Zákonnost

Monitoring zaměstnanců smí být prováděn pouze v souladu se zákonem a, dle čl. 5 odst. 1 písm. a) GDPR, též korektně. Zákonný rámec pro zavedení kontrolních mechanismů za účelem dlouhodobého sledování zaměstnanců je dán v § 316 odst. 2 ZP, jehož problematika je podrobně rozebrána v kapitole 1.4 výše. Bude-li takto prováděný monitoring zaměstnanců představovat zpracovávání jejich osobních údajů (viz kapitola 1.5.1), bude odpovídajícím právním titulem ochrana práv a právem chráněných zájmů zaměstnavatele nebo jiných dotčených osob ve smyslu § 5 odst. 2 písm. e) ZOOÚ, respektive čl. 6 odst. 1 písm. f) GDPR. Pro úplnost, ustanovení § 316 ZP spadá dle mého názoru do úpravy čl. 88 odst. 1 GDPR, podle něhož mohou členské státy právním předpisem stanovit „*konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, zejména za účelem náboru, plnění pracovní smlouvy včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, řízení, plánování a organizace práce, za účelem zajištění rovnosti a rozmanitosti na pracovišti, zdraví a bezpečnosti na pracovišti, ochrany majetku zaměstnavatele nebo majetku zákazníka, dále za účelem individuálního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru*“.

V praxi se nicméně někteří zaměstnavatelé snaží splnění podmínky pro zavedení kontrolních prostředků za účelem sledování zaměstnanců dle § 316 odst. 2 ZP obejít tím, že od zaměstnanců získávají s takovým monitoringem (zpravidla alespoň předchozí) souhlas. Takový postup je ovšem nepřípustný, neboť § 316 ZP představuje kogentní úpravu, od níž se v souladu s ustanovením § 4a odst. 1 ZP nelze odchýlit. Není možné, aby zaměstnavatel nedostatek závažného důvodu ve smyslu § 316 odst. 2 ZP překlenul souhlasem zaměstnance. Navíc, zaměstnanec se nemůže ani svých práv v souvislosti s (neoprávněným) monitoringem platně vzdát; v souladu s § 4a odst. 4 ZP by se k takovému jednání zaměstnance nepřihlíželo. Získaný souhlas zaměstnance by tudíž byl právně bezvýznamný a neúčinný a monitoring zaměstnanců prováděný na jeho základě nezákonný. Kogentnost ustanovení § 316 ZP platí ovšem i opačně; jakmile

zaměstnavatel splní zde stanovenou podmínku, je oprávněn monitorovat své zaměstnance i přes jejich případný výslovný nesouhlas.[63]

V případě nahodilých kontrol zaměstnanců, jež nespadají pod pojem soustavného sledování ve smyslu § 316 odst. 2 ZP, lze uvažovat o dvou možnostech, kdy bude takové zpracování osobních údajů zaměstnanců zákonné – buď tyto kontroly zaměstnavatel ospravedlní jejich nezbytností pro ochranu práv a právem chráněných zájmů svých nebo jiných dotčených osob (ve smyslu § 5 odst. 2 písm. e) ZOOÚ a čl. 6 odst. 1 písm. f) GDPR)[64], nebo k jejich provádění získá souhlas dotčených zaměstnanců (dle § 5 odst. 2 věty první ZOOÚ a čl. 6 odst. 1 písm. a) GDPR).

Získávání souhlasu zaměstnanců se zpracováním osobních údajů ovšem bylo vždy poměrně problematické; mělo by se totiž omezit pouze na případy, kdy má zaměstnanec skutečně svobodnou volbu takový souhlas zaměstnavateli udělit či neudělit, případně jej vzít zpět, aniž by jej za to stíhaly jakékoli následky. Souhlas se zpracováním osobních údajů udělený zaměstnancem zaměstnavateli z obavy ze ztráty zaměstnání či pod hrozbou jiných sankcí by tedy nemohl být považován za svobodně, tj. platně udělený (jak požaduje § 4 písm. n) ZOOÚ a čl. 4 odst. 11 GDPR).[65] Totéž logicky platí v případech, kdy je udělení takového souhlasu podmínkou pro přijetí do zaměstnání, např. jako součást pracovní smlouvy, jak tomu v praxi velice často bývá. V takovém případě totiž zaměstnanec fakticky nemá na vybranou, zda zaměstnavateli souhlas udělí či nikoli, pokud si přeje pracovní smlouvu uzavřít. Většina běžných zaměstnanců není v dostatečně silné pozici na to, aby se zaměstnavatelem úspěšně vyjednávala o obsahu pracovní smlouvy, a dosáhla tak odstranění ustanovení o udělovaném souhlasu. Takto vadné ustanovení pracovní smlouvy dle mého názoru nezhojí ani klauzule o tom, že zaměstnanec má právo souhlas se zpracováním svých osobních údajů kdykoli písemně

---

63 NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 233. ISSN 1210-6410.

64 Oba jmenované právní předpisy zároveň podmiňují zpracování osobních údajů z takového důvodu splněním testu proporcionality; viz kapitola 1.3 výše.

65 Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 8/2001 o zpracování osobních údajů v kontextu zaměstnání (v originále: „*Opinion 8/2001 on the processing of personal data in the employment context*“) ze dne 13. září 2001, s. 23. Viz rovněž recitál 42 GDPR, poslední věta: „*Souhlas by neměl být považován za svobodný, pokud subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout nebo odvolat, aniž by byl poškozen.*“

odvolat (jak toto právo ostatně vyplývá z § 5 odst. 5 ZOOÚ, respektive čl. 7 odst. 3 GDPR); souhlas totiž již od počátku nebyl platně dán, tj. není co odvolávat.

Nové pochybnosti do této problematiky nicméně vnáší GDPR, které v recitálu 43 uvádí, že by „*vyjádření souhlasu nemělo představovat platný právní důvod pro zpracování osobních údajů ve zvláštním případě, kdy mezi subjektem údajů a správcem existuje jasná nerovnováha*“. „Jasná nerovnováha“ je přitom jedním ze čtyř základních znaků závislé práce – tj. vztah nadřízenosti zaměstnavatele a podřízenosti zaměstnance (§ 2 odst. 1 ZP). Zatímco za účinnosti Směrnice 95/46/ES zastávala Pracovní skupina konzistentní stanovisko, že platné udělení souhlasu se zpracováním osobních údajů v pracovněprávních vztazích v zásadě možné je,[66] tento názor s ohledem na GDPR přehodnotila s tím, že osobní údaje zaměstnanců nebude ve většině případů možné na základě souhlasu zpracovávat právě s ohledem na povahu vztahu mezi zaměstnancem a zaměstnavatelem (ledaže zaměstnanci mohou souhlas odvolat bez jakýchkoli negativních důsledků)[67]. Odborná veřejnost se k tomuto tématu taktéž staví velmi opatrně a zaměstnavatelům doporučuje, aby institut souhlasu se zpracováním osobních údajů svých zaměstnancům spíše nevyužívali.[68] Ve většině případů tak neobstojí ani souhlasy udělené před účinností GDPR; v souladu s jeho recitálem 171 by musel být způsob udělení souhlasu v souladu s podmínkami stanovenými GDPR.

I v případě nahodilých kontrol tak lze zaměstnavatelům doporučit, aby se snažili nalézt pro ně důvodné ospravedlnění v podobě jejich nezbytnosti pro ochranu práv a právem chráněných zájmů svých nebo jiných dotčených osob (např. pro již zmíněnou ochranu majetku či bezpečnosti a ochrany zdraví zaměstnanců při práci) a nespoléhali se na

---

66 Dle Pracovní skupiny to platí za předpokladu, kdy jsou dány dostatečné záruky, že byl souhlas zaměstnance udělen svobodně. Viz Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 15/2011 o definici souhlasu (v originále: „*Opinion 15/2011 on the definition of consent*“) ze dne 13. července 2011, s. 13 – 14.

67 Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 6.

68 Např.: (i) White & Case: Unlocking the EU General Data Protection Regulation: A practical Handbook on the EU’s new Data Protection Law, kapitola 8 [online]. Publikováno dne 25. července 2016 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.whitecase.com/publications/article/unlocking-eu-general-data-protection-regulation-practical-handbook-eus-new-data>; (ii) TaylorWessing LLP: Lawful processing of HR data under the GDPR [online]. Publikováno v březnu 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://united-kingdom.taylorwessing.com/globaldatahub/article-processing-of-hr-data-under-the-gdpr.html>.

souhlasy zaměstnanců se zpracováním osobních údajů. V opačném případě by také tyto kontroly mohly být považovány za nezákonné. Na druhou stranu, kritérium nezbytnosti je poměrně přísné; znamená totiž, že ochrany práv a/nebo právem chráněných zájmů zaměstnavatele nelze objektivně dosáhnout jinak – ať už zcela bez zpracování osobních údajů zaměstnanců, nebo jejich zpracováním na základě jiného právního titulu (zpravidla souhlasu, čímž se ovšem dostáváme do bludného kruhu).[69] Zpracování osobních údajů zaměstnance v rámci nahodilé kontroly dodržování zákazu dle § 316 odst. 1 ZP za účelem ochrany majetku zaměstnavatele však zpravidla bude možné považovat za nezbytně nutné pro ochranu práv zaměstnavatele.

(b) Transparentnost a informační povinnost vůči zaměstnancům

Soustavný monitoring zaměstnanců by měl být vždy transparentní. Přestože ze znění § 316 odst. 2 ZP by se dalo teoreticky uvažovat o tom, že ZP umožňuje zaměstnavateli skryté sledování zaměstnanců, pokud je k tomu dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, znění odst. 3 téhož ustanovení tuto možnost fakticky vylučuje. Jsou-li totiž u zaměstnavatele zavedeny kontrolní mechanismy v souladu s § 316 odst. 2 ZP, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění. „Rozsah kontroly“ musí obsahovat konkrétně vymezené údaje, které budou shromažďovány, „způsoby provádění kontroly“ pak podrobnosti typu kdo může tuto kontrolu vykonávat, jakým (technickým) způsobem bude prováděna a za jakých okolností, po jak dlouhou dobu budou shromážděné údaje uchovávány a jak, kdo k těmto údajům bude mít přístup a jakými opatřeními budou tyto údaje zabezpečeny před neoprávněným přístupem a jejich případným zneužitím, apod.

Pokud bude monitoring zaměstnanců představovat též zpracovávání jejich osobních údajů, bude zaměstnavatel jako správce osobních údajů povinen zaměstnance dále v souladu s § 11 ZOOÚ informovat o právu jejich přístupu k osobním údajům, právu na opravu osobních údajů a o právech dle § 21 ZOOÚ (právo požádat o vysvětlení a odstranění závadného stavu v případě, kdy zaměstnanec zjistí nebo se domnívá, že

[69] KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2012, s. 146. ISBN 978-80-7179-226-0.

zpracování jeho osobních údajů probíhá v rozporu se zákonem).[70] S účinností GDPR bude muset být tato informace ještě širší (viz čl. 12 GDPR).

Zásadu transparentnosti nyní výslovně zakotvuje též GDPR v recitálu 39: „*Pro fyzické osoby by mělo být transparentní, že osobní údaje, které se jich týkají, jsou shromažďovány, používány nebo jinak zpracovávány, jakož i v jakém rozsahu tyto osobní údaje jsou či budou zpracovávány.*“ Závazně pak tento požadavek na transparentní způsob zpracovávání osobních údajů ve vztahu k subjektu údajů stanoví v čl. 5 odst. 1 písm. a).

Ačkoli zákon nepřikazuje, aby byla informace o kontrolních mechanismech zaměstnancům podána písemně, část odborné literatury tento názor zastává.[71] Domnívám se, že tato povinnost z výkladu ustanovení § 316 odst. 3 ZP nevyplývá, nicméně s ohledem na prokazování skutečnosti, že zaměstnancům tato informace byla poskytnuta, lze písemnou formu této informace zaměstnavatelům jedině doporučit. V každém případě však musí být z povahy věci taková informace o monitoringu zaměstnancům dána ještě před jeho zahájením. V souladu s recitálem 39 GDPR zásada transparentnosti také vyžaduje, aby byly všechny informace a všechna sdělení týkající se zpracování osobních údajů snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků.

Ustanovení § 316 odst. 3 ZP vyžaduje, aby informace o kontrolních mechanismech byla zaměstnancům podána „přímo“. Může být tudíž obsažena např. v pracovní smlouvě (což ovšem nebude úplně praktické s ohledem na případnou potřebu pozdějších změn), v samostatném dokumentu adresovaném zaměstnanci, případně zprostředkována ústně vedoucím zaměstnancem za přítomnosti svědků, nejlépe s pořízením protokolu o takovém jednání s podpisy všech zúčastněných osob. Rovněž může být obsažena ve vnitřním předpise zaměstnavatele; v takovém případě však musí být tento vnitřní předpis přímo předán zaměstnanci (ideálně oproti jeho potvrzení takového předání)

---

[70] Další informace, které musí správce osobních údajů subjektu osobních údajů sdělit dle § 11 ZOOÚ (tj. informace o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny), by měly být zahrnuty již v informaci podle § 316 odst. 3 ZP.

[71] BĚLINA, Miroslav a kolektiv. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015, xviii, s. 1243. Velké komentáře. ISBN 978-80-7400-290-8.

a nepostačí, pokud bude zaměstnanec na tento vnitřní předpis pouze odkázán[72] (v praxi se totiž velice často v pracovních smlouvách paušálně odkazuje na všechny vnitřní předpisy zaměstnavatele, aniž by tyto kdy byly zaměstnanci skutečně předány).

Požadavek, aby byl monitoring zaměstnanců transparentní, vychází také z dlouhodobé judikatury Evropského soudu pro lidská práva. Podle soudu má zaměstnanec právo legitimně očekávat, že na pracovišti nejsou jeho aktivity sledovány, pokud jej o tom zaměstnavatel předem neinformuje;[73] v citovaných případech však nebyly soukromé aktivity zaměstnanců ze strany zaměstnavatele výslovně zakázány. Určitou výjimku ve své rozhodovací praxi nicméně soud učinil v rozhodnutí ve věci Karin Köpke proti Německu. Šlo o situaci, kdy provozovatel obchodu zaznamenal jisté nesrovnalosti v účetnictví a podezíral své zaměstnance včetně paní Köpke z krádeží. Zaměstnavatel proto nechal prostory obchodu za pomoci detektivní agentury a kamerového systému skrytě sledovat po dobu dvou týdnů a na základě takto pořízených videozáznamů s paní Köpke rozvázal pracovní poměr. Soud se však v tomto případě tentokrát zastal zaměstnavatele. Sice konstatoval, že skrytý monitoring představuje velmi zásadní zásah do soukromí zaměstnance (který takovému sledování nemůže uniknout), ovšem v tomto případě jej připustil. Monitoring byl totiž zaveden z důvodu podezření na páchání krádeží, trval pouze po omezenou dobu a v daném případě nemohl zaměstnavatel efektivně postupovat jiným způsobem, který by do soukromí zaměstnanců zasáhl méně; navíc monitoring pomohl očistit ostatní zaměstnance od podezření z krádeží. Toto rozhodnutí však rozhodně nelze vykládat tak, že skryté sledování zaměstnanců je obecně přípustné, a to, jak dodal sám soud, především s ohledem na míru zásahů do soukromí, které v budoucnu umožní nové a čím dál tím sofistikovanější technologie.[74]

Ani Mezinárodní organizace práce se (zcela očekávaně) nestaví příliš kladně k možnostem skrytého monitoringu zaměstnanců. V čl. 6.14 odst. 2 (právně nezávazného) Kodexu ochrany osobních údajů zaměstnanců uvádí, že skrytý monitoring

---

[72] NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 232. ISSN 1210-6410.

[73] Např. rozsudek Evropského soudu pro lidská práva, stížnost č. 20605/92, ze dne 25. června 1997, Věc Halfordová proti Spojenému království nebo rozsudek Evropského soudu pro lidská práva, stížnost č. 62617/00, ze dne 3. dubna 2007, Věc Coplandová proti Spojenému království.

[74] Rozsudek Evropského soudu pro lidská práva, stížnost č. 420/07, ze dne 5. října 2010, Věc Karin Köpke proti Německu.

by měl být přípustný pouze (i) v případě, kdy jej výslovně umožňují právní předpisy příslušného členského státu, nebo (ii) za předpokladu, že existuje důvodné podezření ze spáchání trestného činu nebo jiného závažného provinění (např. sexuální obtěžování, které nenaplní skutkovou podstatu některého z trestných činů).[75]

Jisté otazníky do požadavku transparentnosti nicméně na úrovni českého práva vnesl Nejvyšší soud v rozsudku sp. zn. 21 Cdo 1771/2011 ze dne 16. srpna 2012. Jednalo se o případ, kdy zaměstnavatel se zaměstnancem okamžitě zrušil pracovní poměr pro porušení povinnosti vyplývající z právních předpisů vztahujících se k jím vykonávané práci zvlášť hrubým způsobem, protože zaměstnanec porušil (nikoli však zcela absolutní) zákaz užívání pracovních prostředků zaměstnavatele tím, že v jednom měsíci strávil v pracovní době celkem 102,97 hodin prohlížením „zakázaných" internetových stránek[76]. Toto množství času přitom představovalo 61,30 % pracovní doby zaměstnance v daném měsíci. Zaměstnavatel takové jednání zaměstnance odhalil tím, že po celý měsíc podrobně sledoval jeho aktivity na internetu, aniž by jej ovšem o takové kontrole předem informoval. Nejvyšší soud nicméně (shodně s oběma soudy nižších stupňů) konstatoval, že v tomto případě nešlo o monitoring zaměstnance ve smyslu § 316 odst. 2 a 3 ZP, ale pouze o přiměřený způsob kontroly dodržování zákazu dle § 316 odst. 1 ZP. Cílem kontroly zaměstnavatele podle Nejvyššího soudu „*nebylo zjišťování obsahu e-mailových zpráv, obsahu SMS nebo MMS, případně odeslaných či přijatých zaměstnancem, nýbrž toliko zjištění, zda zaměstnanec respektuje (a když nerespektuje, tak v jaké míře) zákaz užívat pro svou osobní potřebu výpočetní techniku zaměstnavatele*." Dále soud konstatoval, že: „*o soukromí zaměstnance (o jeho osobnosti) jistě vypovídá i údaj o tom, které internetové stránky sleduje, avšak podstatou kontroly nebylo toto zjištění, nýbrž pouze zjištění, zda zaměstnanec sledoval takové internetové stránky, které s výkonem jeho práce nesouvisely.*"[77] Okamžité

---

[75] MEZINÁRODNÍ ORGANIZACE PRÁCE: *Kodex ochrany osobních údajů zaměstnanců* (v originále: „*Protection of Worker's Personal Data*"). 1. vydání. Ženeva: International Labour Office, 1997, s. 19. ISBN 92-2-110329-3.

[76] Konkrétně se mělo jednat o "*internetové stránky s pochybným či citlivým obsahem nebo stránky typu on-line zpravodajství, sledování TV přes internet nebo poslech rozhlasu přes internet, které mohou nadměrně zatěžovat počítačovou síť a které nesouvisejí s výkonem sjednané práce*". Viz rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1771/2011 ze dne 16. srpna 2012.

[77] Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1771/2011 ze dne 16. srpna 2012. Pro úplnost uveďme, že podle názoru Nejvyššího soudu „*ustanovení § 316 odst. 2 ZP dopadá toliko na případy zvláštní povahy činnosti zaměstnavatele a navíc se vztahuje jen na situace, kdy zaměstnanec buď se*

zrušení pracovního poměru zaměstnance z tohoto důvodu tak bylo podle Nejvyššího soudu v pořádku.

Někteří zaměstnavatelé si výše uvedený rozsudek začali vykládat tak, že skrytý monitoring zaměstnanců je v pořádku. S tím ovšem nelze souhlasit a dle mého názoru není ani zcela správná argumentace Nejvyššího soudu v daném rozhodnutí. Souhlasím s tím, že zaměstnavatel je oprávněn provést kontrolu dodržování zákazu dle § 316 odst. 1 ZP, aniž by musel plnit podmínky dle § 316 odst. 2 a 3 ZP (viz kapitola 1.4 výše). Na druhou stranu, taková kontrola, jež má být dle ZP prováděna přiměřeným způsobem, by dle mého názoru měla být spíše nahodilá (např. v řádech několika dnů, jako tomu bylo v jiném případě řešeném Nejvyšším soudem později[78]) a rozhodně by neměla nést prvky soustavného sledování, jak tomu bylo v posuzovaném případě. Ostatně názor, že zaměstnavatel nesmí sledovat používání webových stránek zaměstnanci bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele, zastává též ÚOOÚ, který se takto vyjádřil ještě před vydáním výše uvedeného rozsudku Nejvyššího soudu.[79] Argumentaci Nejvyššího soudu nicméně podpořil též Ústavní soud, který zaměstnancem podanou ústavní stížnost odmítl pro zjevnou neopodstatněnost, neboť neshledal zásah do práva zaměstnance na soukromí dostatečně intenzivním.[80]

V tomto kontextu je také třeba připomenout rozhodnutí Evropského soudu pro lidská práva ve věci Bărbulescu proti Rumunsku (podrobněji rozebrán v kapitole 1.4 výše), kde zaměstnavatel taktéž skrytě sledoval aktivity zaměstnance na internetovém

---

souhlasem zaměstnavatele používá pro svou osobní potřebu zaměstnavatelovy výrobní a pracovní prostředky, nebo z nějakého důvodu používá u zaměstnavatele své vlastní výrobní a pracovní prostředky včetně výpočetní techniky či telekomunikačního zařízení, a na všechny předměty a projevy soukromé povahy zaměstnance." Podle mého názoru však takové zúžení aplikace § 316 odst. 2 ZP z ničeho nevyplývá a není správné.

78 Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 747/2013 ze dne 7. srpna 2014; v tomto případě byl zaměstnanec skrytě sledován pouze po dobu tří dnů.

79 ÚOOÚ: Stanovisko č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. Únor 2009, s. 4.

80 „*Ústavní soud neshledal důvodu, pro který by takto řádně odůvodněný závěr Nejvyššího soudu bylo možno označit za svévolný či extrémní, resp. excesivní, neboť má racionální základ a je logicky a srozumitelně odůvodněn, což je z pohledu zásad ústavněprávního přezkumu rozhodné*." … „*Zásah takové intenzity ani s přihlédnutím ke stanovisku č. 2/2009 Úřadu pro ochranu osobních údajů do práva na ochranu soukromí stěžovatele Ústavní soud neshledal*." Viz usnesení Ústavního soudu sp. zn. I. ÚS 3933/12 ze dne 7. listopadu 2012.

komunikátoru. V tomto případě však skryté sledování trvalo pouze po dobu 9 dnů.[81] Domnívám se, že ke zjištění, zda zaměstnanec navštěvuje internetové stránky pro svou soukromou potřebu bez předchozího svolení, by sledování v řádech dnů mělo zaměstnavateli bohatě stačit. Skryté sledování zaměstnance po dobu jednoho měsíce podle mého názoru představuje velmi intenzivní zásah do jeho soukromí, navzdory názoru Ústavního soudu.

Poměrně striktní výklad k otázce transparentnosti především s ohledem na znění GDPR zaujímá Pracovní skupina; dle jejího nedávného stanoviska musejí být zaměstnanci informováni o existenci jakéhokoli zavedeného monitoringu, zejména s ohledem na nově dostupné technologie, jež umožňují zpracovávání velkého množství dat skrytým způsobem.[82]

(c) Omezení účelu a rozsahu zpracovávaných osobních údajů

V souladu s § 5 odst. 1 písm. a) ZOOÚ je každý správce povinen stanovit účel, k němuž mají být osobní údaje zpracovány; zpracovávání osobních údajů bez předem stanoveného účelu nebo pro neomezené účely by bylo v rozporu se zákonem. V případě soustavného monitoringu zaměstnanců dle § 316 odst. 2 ZP musí účel zpracování osobních údajů odpovídat důvodu, pro který byly příslušné kontrolní mechanismy zavedeny. Bude se tedy jednat typicky o ochranu majetku zaměstnavatele, ochranu bezpečnosti a zdraví zaměstnanců při práci, síťovou bezpečnost, ochranu utajovaných skutečností, bankovního nebo obchodního tajemství, důvěrných informací nebo know-how, apod. Obdobné účely by měl zaměstnavatel identifikovat i pro nahodilé kontroly zaměstnanců (nespadající pod § 316 odst. 2 ZP), aby bylo možné zpracovávat osobní údaje bez jejich souhlasu; bude však třeba naplnit kritérium nezbytnosti takového zpracovávání pro ochranu práv a právem chráněných zájmů zaměstnavatele ve smyslu § 5 odst. 2 písm. e) ZOOÚ (k tomu viz výše bod (a) této kapitoly).

Ustanovení § 5 odst. 1 písm. d) ZOOÚ stanoví, že správce je povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro

---

[81] Rozsudek Evropského soudu pro lidská práva, stížnost č. 61496/08, ze dne 12. ledna 2016, Věc Bărbulescu proti Rumunsku.

[82] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 8.

naplnění stanoveného účelu; dle písm. f) téhož ustanovení je pak správce povinen osobní údaje zpracovávat pouze v souladu s účelem, k němuž byly shromážděny. Obdobně podle čl. 5 odst. 1 písm. b) GDPR musejí být osobní údaje shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; dle písm. c) téhož ustanovení pak musejí být osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány. V posledním zmíněném bodě je úprava GDPR oproti předchozí úpravě přísnější; Směrnice 95/46/ES pouze požadovala, aby údaje nepřesahovaly míru s ohledem pro účely, pro které jsou shromažďovány a/nebo dále zpracovávány.

Zaměstnavatel by tak měl předem nejen vymezit účel, pro který k monitoringu a souvisejícímu zpracovávání osobních údajů zaměstnanců dochází, ale též rozsah údajů, které hodlá pro stanovený účel zpracovávat. Příslušný účel je třeba vymezit dostatečně určitě a přitom srozumitelně tak, aby jej nebylo možné zaměnit za jiný. Pojem „legitimní účel“ je přitom třeba chápat poměrně široce; takový účel musí být v souladu nejen s obecně závaznými právními předpisy, ale též se základními lidskými právy (tj. zejména právem na ochranu soukromí) a všeobecnými právními principy (typicky s dobrými mravy).[83]

Jiné než ke stanovenému účelu nezbytné osobní údaje nesmí zaměstnavatel shromažďovat a zpracovávat; monitoring musí být prováděn takovým způsobem, aby v souladu se zásadou proporcionality představoval co nejmenší zásah do soukromí zaměstnanců. Pokud tedy např. zaměstnavatel zakáže zaměstnancům navštěvovat vymezené sociální sítě z pracovního počítače v pracovní době, ale mimo pracovní dobu jim takové jednání umožní, přičemž za účelem kontroly tohoto zákazu monitoruje, zda zaměstnanci tyto sociální sítě navštěvují, pak není oprávněn tak činit mimo pracovní dobu, přestože by z takových výsledků monitoringu nevyvozoval pro zaměstnance žádné důsledky.[84]

---

[83] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 03/2013 o omezení účelem (v originále: „*Opinion 03/2013 on purpose limitation*“) ze dne 2. dubna 2013, s. 17 – 20.

[84] V tomto případě by v praxi bylo samozřejmě mnohem efektivnější a vhodnější přístup na vymezené sociální sítě jednoduše blokovat v rámci internetového připojení zaměstnavatele.

Osobní údaje shromážděné pro určitý účel lze užít pro jiný účel pouze za předpokladu, že je tento s původním účelem slučitelný. Ovšem posouzení takové slučitelnosti, které by správce měl učinit předtím, než shromážděné údaje pro nový účel použije, nebude v praxi snadné. Dle recitálu 50 GDPR (jenž ve skutečnosti pouze shrnuje závěry Pracovní skupiny přijaté ke znění Směrnice 95/46/ES) je třeba vzít v úvahu zejména následující kritéria: (i) jakoukoli vazbu mezi původním a novým účelem (tj. např. zda nový účel logicky navazuje na původní nebo v něm případně byl již od počátku implicitně obsažen)[85]; (ii) kontext, v němž byly osobní údaje shromážděny, zejména přiměřená očekávání ohledně dalšího použití osobních údajů, která subjekty údajů mají na základě svého vztahu se správcem; (iii) povahu osobních údajů a důsledky zamýšleného dalšího zpracování pro subjekty údajů (pokud by byl tento dopad zvláště negativní, nový účel zpracování s původním účelem slučitelný zpravidla nebude)[86]; a konečně (iv) existenci vhodných záruk jak během původních, tak během zamýšlených dalších operací zpracování, jež správce přijal k zajištění spravedlivého zpracování a k vyloučení jakéhokoli nepřípustného dopadu na subjekt údajů (např. kompletní či částečná pseudonymizace[87] nebo anonymizace[88] údajů, vyšší zabezpečení údajů apod.).[89]

Jako příklad neslučitelnosti nového účelu zpracování osobních údajů s původním účelem uvádí Pracovní skupina následující scénář: kamerový systém, který zaměstnavatel instaloval ve vstupu do areálu za účelem jeho zabezpečení před vstupem nepovolaných osob, zachytí kromě jiného recepční, jak se opakovaně vzdaluje ze svého pracoviště a neplní své pracovní povinnosti. Po provedení „testu slučitelnosti“ dle výše

---

85 Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 03/2013 o omezení účelem (v originále: „*Opinion 03/2013 on purpose limitation*“) ze dne 2. dubna 2013, s. 24.

86 Tamtéž, s. 25 – 26.

87 Pojem pseudonymizace je definován v čl. 4 odst. 5 GDPR jako „*zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě*“. V ZOOÚ tento pojem definován není.

88 Tento pojem není v ZOOÚ ani v GDPR definován; anonymizované údaje jsou však takové údaje, které s danou osobou nesouvisejí nebo byly poskytnuty anonymně takovým způsobem, že daná osoba již na jejich základě není identifikovatelná.

89 Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 03/2013 o omezení účelem (v originále: „*Opinion 03/2013 on purpose limitation*“) ze dne 2. dubna 2013, s. 26 – 27.

uvedených kritérií by měl nicméně zaměstnavatel dojít k závěru, že z takto pořízených záznamů nemůže vůči recepční vyvozovat žádné důsledky.[90]

Na druhou stranu, pokud by zaměstnavatel instaloval do svých prostor kamerový systém za účelem ochrany majetku a prevence kriminality a následně by jeho prostřednictvím pořídil záznam svých zaměstnanců, kteří po skončení pracovní doby na pracovišti pořádají oslavu, požívají alkoholické nápoje a v rozporu s požárními předpisy kouří, dovozuje Morávek, že by tyto záznamy mohly být použity též k prokázání hrubého porušení pracovní kázně těchto zaměstnanců. Přestože byly záznamy striktně vzato pořízeny k jinému účelu, lze s ohledem na princip proporcionality a možnou míru očekávání soukromí konstatovat, že využití těchto záznamů pro účely prokázání hrubého porušení pracovní kázně je legitimní. Ostatně v důsledku popsaného jednání zaměstnanců mohla na majetku zaměstnavatele vzniknout značná škoda (např. pokud by došlo k požáru), čímž se dostáváme k původně deklarovanému účelu zpracování osobních údajů.[91]

(d) Přesnost údajů

Dle čl. 5 odst. 1 písm. d) GDPR je zaměstnavatel jako správce osobních údajů oprávněn zpracovávat pouze přesné údaje, které je povinen v případě potřeby aktualizovat; nepřesné údaje mají být bezodkladně vymazány nebo opraveny. V ZOOÚ najdeme obdobné ustanovení v § 5 odst. 1 písm. c). V kontextu monitoringu zaměstnanců nicméně tato zásada z povahy věci zpravidla stěžejní nebude. Je však vhodné připomenout právo subjektu údajů žádat po správci osobních údajů provedení opravy nepřesných údajů dle § 21 odst. 1 písm. b) ZOOÚ (respektive dle čl. 16 GDPR).

(e) Časové omezení ukládání osobních údajů a právo subjektu údajů být zapomenut

Dle čl. 5 odst. 1 písm. e) GDPR je zaměstnavatel jako správce osobních údajů oprávněn ukládat osobní údaje umožňující identifikaci zaměstnanců po dobu nikoli delší, než je nezbytné pro účely, pro které tyto údaje zpracovává; v souladu s recitálem 39 GDPR má

---

90 Tamtéž, s. 56.

91 MORÁVEK, Jakub. Kdy lze jako důkazní prostředek připustit záznam z kamerového systému? *Právní rozhledy*. 2011, roč. 19, č. 13, s. 458, 462 – 463. ISSN 1210-6410.

být přitom tato doba omezena na nezbytné minimum. V ZOOÚ je úprava týkající se možné doby zpracování osobních údajů obsažena v § 5 odst. 1 písm. e).

Zaměstnavatel by tudíž měl pravidelně vyhodnocovat, zda jím uložené osobní údaje zaměstnanců ještě nezbytně potřebuje zpracovávat; pokud nikoli, měl by takové údaje buď co nejdříve zlikvidovat, nebo anonymizovat či pseudonymizovat tak, aby tyto údaje již identifikaci zaměstnanců neumožňovaly.

GDPR též výslovně zakotvuje právo subjektu údajů „být zapomenut“. Dle čl. 17 GDPR má subjekt údajů právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají. Správce má pak povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán některý z vymezených důvodů. Jedním z nich je situace, kdy osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány, nebo případ, kdy subjekt údajů odvolá souhlas se zpracováním osobních údajů, aniž by byl současně dán jiný právní důvod pro jejich zpracování. Právo být zapomenut nicméně již před úpravou v GDPR dovodil Soudní dvůr Evropské unie ve věci stížnosti pana Costejy Gonzáleze proti společnosti Google, kdy uznal jeho právo požadovat, aby společnost Google neposkytovala informace o jeho osobě široké veřejnosti prostřednictvím zahrnutí jeho jména do seznamu výsledků vyhledávání poté, kdy tyto informace přestaly být přesné a relevantní, respektive se staly excesivními s ohledem na uvedené účely a uplynulý čas.[92]

Zaměstnavatelé by proto měli počítat s eventualitou, že zaměstnanci budou žádat výmaz svých osobních údajů právě s ohledem na právo být zapomenut, zejména v souvislosti se skončením pracovního poměru.

(f) Zabezpečení údajů

Dle čl. 5 odst. 1 písm. f) GDPR musejí být osobní údaje zpracovávány způsobem, který zajistí jejich náležité zabezpečení, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před

[92] Rozsudek Soudního dvora (velkého senátu) ze dne 13. května 2014 ve věci C-131/12, Google Spain SL a Google Inc. v. Agencia Espanola de Protección de Datos (AEPD) a Mario Costeja González. V daném případě šlo o situaci, kdy se jméno stěžovatele zobrazovalo ve vyhledávači Google s odkazem na internetové články s uveřejněním dražby jeho nemovitostí zabavených v důsledku dluhů na sociálním zabezpečení. K dražbě samotné přitom došlo dlouhých 12 let před podáním stížnosti pana Gonzáleze k Soudnímu dvoru.

náhodnou ztrátou, zničením nebo poškozením. Podrobnější pravidla za účelem naplnění této zásady jsou upravena v čl. 32 GDPR[93]. Na úrovni ZOOÚ jsou povinnosti zaměstnavatele při zabezpečení osobních údajů zakotveny v § 13; dle § 13 odst. 1 ZOOÚ je správce povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů; tato povinnost trvá samozřejmě i po ukončení zpracovávání osobních údajů.

Před spuštěním monitoringu by měl zaměstnavatel předně posoudit možná rizika ve vztahu ke shromažďovaným osobním údajům a nastavit vhodná bezpečnostní opatření a mechanismy, jež by tato rizika pomáhala minimalizovat. Tuto analýzu i přijatá technicko-organizační opatření je dle § 13 odst. 2 ZOOÚ povinen zdokumentovat. Rizika, která je zaměstnavatel povinen při posuzování úrovně bezpečnosti zvážit, demonstrativně uvádí čl. 32 odst. 2 GDPR: „*náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim*“. Dle stávajícího znění § 13 odst. 3 ZOOÚ se rizika týkají „*a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům; b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování; c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje; a d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány*.“ Pokud zaměstnavatel zpracovává osobní údaje automatizovaně, jak tomu zpravidla při monitoringu zaměstnanců bývá, je dle § 13 odst. 4 ZOOÚ dále povinen „*a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby; b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;*

[93] Zde jsou i příkladmo uvedena některá vhodná technická a organizační opatření, jež by měl správce údajů zavést: (i) pseudonymizace a šifrování osobních údajů, (ii) schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování, (iii) schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; a (iv) proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány a d) zabránit neoprávněnému přístupu k datovým nosičům."

Bezpečnostní opatření by tak měla směřovat proti rizikům hrozícím zevnitř (např. jednání zaměstnanců, ať už úmyslné či nedbalostní, technické selhání) i zvenčí (např. neoprávněný přístup třetích osob, živelní pohromy). Zaměstnavatel by proto především měl (i) řádně zabezpečit prostory, v nichž dochází ke shromažďování a zpracování osobních údajů (typicky pomocí bezpečnostních zámků, mříží a pultu centrální ochrany, jak uvádí formulář ÚOOÚ k oznámení o zpracování osobních údajů, ale též např. pomocí kamerového systému), (ii) přijmout odpovídající opatření v personální oblasti (např. minimalizace okruhu zaměstnanců, kteří mají k osobním údajům přístup[94], podrobné vymezení jejich úkolů a odpovědností, přijetí odpovídajícího vnitřního předpisu[95] a bezpečnostních směrnic, pravidelné školení zaměstnanců a kontrola plnění jejich povinností[96], sjednání povinnosti mlčenlivosti v pracovních smlouvách se

---

[94] Z rozhodovací praxe ÚOOÚ: „*V případě účastníka řízení je zřejmé, že nepřijal dostatečná opatření pro zabezpečení osobních údajů, v důsledku čehož měl každý zaměstnanec, který byl povinen pracovat s informačním systémem, přístup k osobním údajům všech vězněných osob, a to i v případě, kdy tento přístup nebyl nezbytný k výkonu jeho práce. Pouhé vymezení povinností, zákazů a oprávnění při práci s informačním systémem ve vnitřním předpise nelze považovat za veškeré možné úsilí, které mohl účastník řízení vynaložit k tomu, aby zabránil neoprávněnému přístupu k osobním údajům.*" Viz ÚOOÚ: K zabezpečení osobních údajů v informačním systému (přístupová oprávnění zaměstnanců) [online]. Publikováno dne 18. června 2014 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/k-nbsp-zabezpeceni-osobnich-udaju-v-nbsp-informacnim-systemu-pristupova-opravneni-zamestnancu/d-10895/p1=1483>.

[95] Z rozhodovací praxe ÚOOÚ: „*V případě účastníka řízení ze spisového materiálu vyplývá, že se sice jednalo o ojedinělý incident vzniklý pravděpodobně špatným vzájemným informováním dvou jeho zaměstnanců, přesto po posouzení všech okolností dospěl správní orgán k závěru, že liberační ustanovení v tomto případě naplněno nebylo. Ze spisového materiálu Policie České republiky totiž vyplývá, že zaměstnankyně nebyla ze strany účastníka řízení žádným způsobem proškolena v oblasti nakládání s osobními údaji, vnitřní předpis upravující ochranu práv klientů byl účastníkem řízení přijat až po předmětném incidentu. Jako vynaložení veškerého úsilí nelze ani hodnotit skutečnost, že osobní údaje uložené v notebooku nebyly žádným způsobem chráněny před neoprávněným zpracováním přístupovým heslem.*" Viz ÚOOÚ: K zabezpečení osobních údajů zpracovávaných výpočetní technikou [online]. Publikováno dne 21. března 2013 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/k-zabezpeceni-osobnich-udaju-zpracovavanych-vypocetni-technikou/d-1583/p1=1483>.

[96] Z rozhodovací praxe ÚOOÚ: „*Za opatření ve smyslu § 13 odst. 1 zákona o ochraně osobních údajů lze považovat i pokyny určené zaměstnancům účastníka řízení v interních předpisech, které účastník řízení předložil, nicméně samotná existence těchto předpisů není dostačující v případě, kdy tyto pokyny nejsou v praxi dodržovány a jejich dodržování důsledně kontrolováno.*" Viz ÚOOÚ: K dodržování povinnosti přijmout a provést bezpečností opatření k ochraně osobních údajů v soukromoprávní sféře [online]. Publikováno dne 21. března 2013 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/k-dodrzovani-povinnosti-prijmout-a-provest-bezpecnosti-opatreni-k-ochrane-osobnich-udaju-v-soukromopravni-sfere/d-1598>.

zaměstnanci, kteří mají k osobním údajům přístup, apod.), a (iii) zabezpečit informační systémy a datová úložiště (např. nastavení víceúrovňových přístupových hesel pro každou oprávněnou osobu, vhodná antivirová ochrana, šifrování, pravidelné zálohování dat, zaznamenávání všech přístupů k osobním údajům a jakékoli manipulace s nimi, apod.).

Při nastavování bezpečnostních opatření by měl zaměstnavatel případně zvážit využití mezinárodních a/nebo českých technických norem, např. normu ČSN ISO/IEC 27005 (369790) - Řízení rizik bezpečnosti informací. Jak konstatoval Nejvyšší správní soud, i v oblasti bezpečnostních opatření existují určité standardy, které lze realizovat, aniž by musely být výslovně stanoveny zákonem; ke každé technologii existuje soubor bezpečnostních opatření považovaný za standard, přičemž tento by měl představovat pouze nutné minimum opatření, jež je třeba přijmout.[97] Využije-li zaměstnavatel aktuálně platné technické normy (s přihlédnutím k vlastním individuálním podmínkám), bude v případě sporu snadněji prokazovat, že jím přijatá technicko-organizační opatření na poli zabezpečení osobních údajů bylo možné považovat v souladu s obecně uznávanými pravidly za dostačující.[98]

Novinkou, kterou správcům přináší GDPR v čl. 32 odst. 3, je možnost doložit soulad s požadavky na řádné zabezpečení osobních údajů dodržováním kodexu chování dle čl. 40 GDPR nebo uplatňováním schváleného mechanismu pro vydávání osvědčení dle čl. 42 GDPR.

Návrhy kodexů chování mají být v budoucnu vypracovány sdruženími nebo jinými subjekty zastupujícími různé kategorie správců nebo zpracovatelů. Následně musejí být

---

[97] Rozsudek Nejvyššího správního soudu sp. zn. 3 As 21/2005 ze dne 10. května 2006. V daném případě stěžovatelka neúspěšně namítala, že § 13 ZOOÚ není dostatečně konkrétní, co se týče opatření, jež má správce přijmout za účelem zabezpečení osobních údajů.

[98] Z rozhodovací praxe ÚOOÚ: „*Účastník řízení uvedl, že má přijatá technicko-organizační opatření jak v „minimálním standardu“, který má vyplývat z formuláře pro plnění oznamovací povinnosti, tak přijal i opatření další. V důsledku toho, kromě lidského selhání některého ze svých zaměstnanců, vylučuje možnost neoprávněného přístupu a zneužití osobních údajů… Z vyjádření účastníka řízení vyplývá, že ani on sám není schopen určit, jakým způsobem ke zpřístupnění osobních údajů došlo. Už sama tato skutečnost dle správního orgánu znamená, že účastník řízení nevynaložil veškeré úsilí, aby porušení právní povinnosti zabránil. Jinými slovy, pokud účastník řízení argumentuje lidským selháním, přičemž není schopen sám toto lidské selhání následně odhalit a současně nemá přijatá taková opatření, aby riziko lidského selhání minimalizoval, nelze konstatovat, že by vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil.*“ Viz ÚOOÚ: K zabezpečení osobních údajů [online]. Publikováno dne 18. dubna 2013 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/k-zabezpeceni-osobnich-udaju/d-1750/p1=1483>.

předloženy ke schválení příslušnému dozorovému úřadu (v ČR ÚOOÚ) nebo Sboru, pokud se má návrh kodexu týkat více členských států. Na základě stanoviska Sboru může Evropská komise prohlásit vypracovaný kodex chování za všeobecně platný v rámci celé Evropské unie. Posláním kodexů chování má být upřesnění uplatňování ustanovení GDPR nejen s ohledem na zabezpečení osobních údajů, ale s ohledem na soulad prováděného zpracování osobních údajů s GDPR jako celkem. Dodržování kodexů ze strany správců a zpracovatelů osobních údajů mají kromě dozorových úřadů kontrolovat též další subjekty, které k tomu budou dozorovými úřady akreditovány. Pomyslnou vlaštovkou v této oblasti je kodex chování, který dne 27. ledna 2017 vydala za tímto účelem nově utvořená skupina poskytovatelů cloudových služeb působících v Evropě, skupina CISPE (z anglického *Cloud Infrastructure Services Providers*).[99] Lze očekávat, že v budoucnu vznikne celá řada dalších asociací sdružujících podnikatele dle různých oborů podnikání, které budou vydávat kodexy chování s ohledem na jejich specifické potřeby.

GDPR dále předpokládá vydávání osvědčení o ochraně údajů a udělování pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu zpracování s GDPR. Tyto se mohou vztahovat na konkrétní produkt, službu, ale i na celý proces zpracovávání osobních údajů prováděný správcem. Osvědčení, pečetě a známky mají správcům a zpracovatelům udělovat k tomu akreditované subjekty[100] nebo přímo příslušné dozorové úřady nejvýše na dobu tří let (s možností opakovaného udělení). Získáním osvědčení se nicméně nesnižuje odpovědnost správců a zpracovatelů za soulad s GDPR, ani nejsou nijak dotčeny pravomoci dozorových úřadů, co se týče provádění kontrol u správců/zpracovatelů. Proces vydávání osvědčení na poli ochrany

---

99 Kodex je dostupný z WWW: <https://cispe.cloud/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf>.

100 Dle čl. 43 odst. 1 GDPR mohou subjekty tuto akreditaci získat buď od příslušného dozorového úřadu, nebo od vnitrostátního akreditačního orgánu určeného v souladu s (i) Nařízením Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93, (ii) normou EN-ISO/IEC 17065/2012 (Posuzování shody - Požadavky na orgány certifikující produkty, procesy a služby) a s (iii) dodatečnými požadavky stanovenými příslušným dozorovým úřadem. ÚOOÚ se rozhodl určit za vnitrostátní akreditační orgán Český institut pro akreditaci, o.p.s. (IČO: 256 77 675); viz ÚOOÚ: Věstník Úřadu pro ochranu osobních údajů. Částka 73, srpen 2017, s. 4131.

osobních údajů je již v některých členských státech Evropské unie zavedený[101]; zatím však tato osvědčení směřovala logicky pouze na příslušnou vnitrostátní úpravu. Je otázkou, jak hojně bude tato novinka využívána; někteří autoři jsou v tomto směru poměrně skeptičtí, už s ohledem na nákladnost procesu získání osvědčení a nedostatečnou motivaci takové osvědčení získat (vzhledem k tomu, že odpovědnost za zpracování zůstává v plném rozsahu na správcích/zpracovatelích).[102] Používání pečetí a známek nicméně může být využitelné marketingově vůči zákazníkům; v kontextu monitoringu zaměstnanců si jejich časté užívání příliš nedovedu představit (snad jen velmi teoreticky jako určitý benefit představovaný uchazečům o zaměstnání).

Další novinkou, kterou přinese GDPR, bude povinnost hlásit případy porušení zabezpečení osobních údajů. Oznamovací povinnost bude mít správce vůči ÚOOÚ dle čl. 33 GDPR a za určitých podmínek též vůči samotným subjektům údajů dle čl. 34 GDPR.

K ohlášení ÚOOÚ musí dojít bez zbytečného odkladu, pokud možno do 72 hodin od okamžiku, kdy se o porušení zabezpečení osobních údajů správce dozvěděl, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob (pokud je ohlášení učiněno později, musí být současně uvedeny důvody tohoto zpoždění). Náležitosti ohlášení jsou uvedeny v čl. 33 odst. 3 GDPR.[103] Nepravděpodobnost rizika pro práva a svobody fyzických osob by přitom správce měl být schopen v souladu se zásadou odpovědnosti (viz bod (g) níže) doložit (recitál 85 GDPR).

---

[101] Konkrétně v Nizozemsku, Maďarsku, Německu, Spojeném království Velké Británie a Severního Irska a ve Francii. Viz LACHAUD, Erich. Why the certification process defined in the General Data Protection Regulation cannot be successful. *Computer Law & Security Review*. 2016, roč. 32, č. 6, s. 815. ISSN 0267-3649.

[102] LACHAUD, Erich. Why the certification process defined in the General Data Protection Regulation cannot be successful. *Computer Law & Security Review*. 2016, roč. 32, č. 6, s. 825 – 826. ISSN 0267-3649.

[103] Ohlášení musí přinejmenším obsahovat „*a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů; b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace; c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů; d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů*.“

Oznamovací povinnost přímo vůči subjektu údajů má správce tehdy, jestliže je pravděpodobné, že daný případ porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, ledaže „*a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování* (pozn. dle ÚOOÚ též pseudonymizace údajů bez vazby na subjekt údajů)[104]*; b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví; c) vyžadovalo by to nepřiměřené úsilí; v takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření*.“ Oznámení by mělo být dle recitálu 86 GDPR provedeno bez zbytečného prodlení a případně v úzké spolupráci s příslušným dozorovým úřadem, respektive v souladu s jeho pokyny.

Co se týče posuzování rizika porušení zabezpečení, je dle ÚOOÚ třeba vycházet zejména z kategorie dotčených osobních údajů, charakteru porušení zabezpečení (riziko např. zvyšuje situace, kdy narušitel jednal úmyslně) a počtu dotčených subjektů údajů. V této souvislosti ÚOOÚ doporučuje, aby správci zvážili šifrování nebo pseudonymizaci osobních údajů, které je mohou z ohlašovací povinnosti vyvázat.[105]

Z výše uvedeného výkladu vyplývá, že problematika zabezpečení osobních údajů je velmi komplexní; bez zdatného IT oddělení nebo efektivního outsourcingu IT služeb prakticky nebude možné monitoring zaměstnanců se zpracováním osobních údajů provádět.

(g) Odpovědnost zaměstnavatele jako správce osobních údajů a sankce za neoprávněný monitoring zaměstnanců

Dalším principem, který pro správce bude vyplývat z GDPR, je výslovná odpovědnost za dodržení všech výše uvedených zásad zpracování osobních údajů a povinnost být schopen tuto skutečnost doložit (čl. 5 odst. 2 GDPR). Z čl. 6 odst. 2 Směrnice 95/46/ES zaznával pouze požadavek, aby správce zajistil dodržování všech zásad zpracování

[104] ÚOOÚ: Obecné nařízení o ochraně osobních údajů v otázkách a odpovědích [online]. Publikováno dne 25. května 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-v-otazkach-a-odpovedich/d-23790/p1=3938>.

[105] Tamtéž.

osobních údajů; v tomto směru je tedy znění GDPR důraznější. Správci údajů by tak měli důsledně dodržovat veškeré zásady zpracování osobních údajů a své postupy v této oblasti řádně dokumentovat.

V soukromoprávní rovině bude zaměstnavatel jako správce osobních údajů dle čl. 82 GDPR odpovídat zaměstnancům za hmotnou i nehmotnou újmu, která jim vznikne v důsledku monitoringu se zpracováním osobních údajů, jež nebude plně v souladu s GDPR. Za zpracování, které porušuje GDPR, se má přitom dle recitálu 146 GDPR považovat rovněž zpracování, které porušuje též právní předpisy jednotlivých členských států. Povinnosti nahradit újmu se dle čl. 82 odst. 3 GDPR zaměstnavatel zprostí, pouze pokud prokáže, že za událost, která ke vzniku újmy vedla, nenese žádným způsobem odpovědnost. Pojem „újma" by přitom dle recitálu 146 GDPR měl být vykládán široce a měl by se opírat o judikaturu Soudního dvora Evropské unie. Soukromoprávní nároky zaměstnance dle českého práva v souvislosti s neoprávněným monitoringem jsou podrobněji rozebrány v kapitole 3.4 níže.

Ve veřejnoprávní rovině pak hrozí zaměstnavateli za porušení povinností v oblasti zpracování osobních údajů pokuty ze strany ÚOOÚ. Do účinnosti GDPR představuje horní hranici možných pokut částka ve výši 10 000 000 Kč.[106] S účinností GDPR nicméně dojde k razantnímu zvýšení horních sazeb pokut, což vyvolalo mezi podnikateli i ve sdělovacích prostředcích řadu negativních reakcí. Nová horní hranice možných pokut tak činí 20 000 000 EUR, nebo, jedná-li se o podnik, částku odpovídající 4 % celkového ročního obratu celosvětově za předchozí rozpočtový rok, podle toho, která z obou částek je vyšší. GDPR však samozřejmě respektuje zásady správního trestání a správního uvážení; v čl. 83 odst. 1 požaduje, aby byly pokuty v každém jednotlivém případě účinné, přiměřené a odrazující. Pokuty mají být ukládány podle okolností každého jednotlivého případu se zohledněním polehčujících a přitěžujících okolností uvedených v čl. 83 odst. 2 GDPR.[107] Mimo jiné i s ohledem na

[106] Dle vyjádření ÚOOÚ nicméně nejvyšší dosud (respektive do 25. května 2017, kdy bylo toto vyjádření publikováno) uložená pokuta nedosahovala ani poloviny této částky. Viz ÚOOÚ: Desatero omylů o obecném nařízení (GDPR) [online]. Publikováno dne 25. května 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/desatero-omylu-o-obecnem-narizeni-gdpr/d-23799/p1=3938>.

[107] Např. povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena, kroky podniknuté správcem ke zmírnění škod, míra odpovědnosti správce s přihlédnutím k technickým

judikaturu Ústavního soudu ohledně ukládání nepřiměřených (a tudíž likvidačních) sankcí[108] proto nelze ani po účinnosti GDPR očekávat na úrovni České republiky příliš razantní zvýšení skutečně ukládaných pokut; na tuto skutečnost ostatně upozorňuje též ÚOOÚ.[109]

S účinností od 29. července 2017 může být zaměstnavateli také uložena pokuta ze strany Státního úřadu inspekce práce v případě, že neoprávněně monitoruje své zaměstnance, čili „*naruší soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele některým ze způsobů uvedených v § 316 odst. 2 zákoníku práce*" (§ 11a odst. 1 písm. a) zákona o inspekci práce, respektive § 24a odst. 1 písm. a) zákona o inspekci práce pro zaměstnavatele – právnické osoby), nebo v případě, kdy „*neinformuje zaměstnance o rozsahu kontroly a o způsobech jejího provádění podle § 316 odst. 3 zákoníku práce*" (§ 11a odst. 1 písm. b) zákona o inspekci práce, respektive § 24a odst. 1 písm. b) zákona o inspekci práce pro zaměstnavatele – právnické osoby). Za přestupek dle první jmenované skutkové podstaty lze zaměstnavateli (bez ohledu na skutečnost, zda je zaměstnavatel fyzickou či právnickou osobou) uložit pokutu až do výše 1 000 000 Kč, za druhý jmenovaný přestupek až do výše 100 000 Kč. Před začleněním těchto skutkových podstat do zákona o inspekci práce mohly orgány inspekce práce nejvýše konstatovat porušení ZP a uložit zaměstnavateli opatření k odstranění zjištěných nedostatků což, jak konstatuje důvodová zpráva k příslušné novele zákona o inspekci práce, nebylo dostatečně efektivní a odrazující. Zákonodárce tak konečně vyslyšel Veřejného ochránce práv, který na takto nedostatečnou právní úpravu dlouhodobě upozorňoval.[110] Nyní je tedy otázkou, jak hojně bude Státní úřad inspekce práce toto své nové oprávnění využívat.

Co se týče odpovědnosti za výše uvedené přestupky, zaměstnavateli – fyzické osobě, bude třeba prokázat zavinění, a to dle § 15 odst. 1 ZOP alespoň z nedbalosti.

---

a organizačním opatřením jím zavedeným, kategorie osobních údajů dotčené daným porušením, dodržování schválených kodexů chování nebo schváleného mechanismu pro vydávání osvědčení, apod.

[108] Např. Nález Ústavního soudu sp. zn. Pl. ÚS 52/13 ze dne 9. září 2014.

[109] ÚOOÚ: Desatero omylů o obecném nařízení (GDPR) [online]. Publikováno dne 25. května 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/desatero-omylu-o-obecnem-narizeni-gdpr/d-23799/p1=3938>.

[110] Vládní návrh zákona, kterým se mění zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a další související zákony. Sněmovní tisk č. 911/0, s. 79 – 80. Tento návrh zákona byl vyhlášen ve Sbírce zákonů dne 14. července 2017 pod č. 206/2017 Sb.

Zaměstnavatel – právnická osoba, nebude za přestupek dle § 21 odst. 1 ZOP odpovídat pouze tehdy, prokáže-li, že vynaložil veškeré úsilí, které bylo možno požadovat, aby přestupku zabránil. Dle odst. 2 téhož ustanovení se ovšem odpovědnosti nezprostí, pokud z jeho strany nebyla vykonávána povinná nebo potřebná kontrola nad fyzickou osobou, která se za účelem posuzování odpovědnosti zaměstnavatele za přestupek považuje za osobu, jejíž jednání je přičitatelné zaměstnavateli – právnické osobě, nebo nebyla učiněna nezbytná opatření k zamezení nebo odvrácení přestupku.

Novinkou, kterou GDPR přináší, je povinnost provést posouzení vlivu na ochranu osobních údajů dle čl. 35, pokud je pravděpodobné, že určitý druh zpracování osobních údajů, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob. Posouzení by přitom mělo být provedeno před zahájením zpracování a za jeho řádné provedení plně odpovídá správce. GDPR v čl. 35 odst. 3 příkladmo uvádí situace, kdy je nutné posouzení vlivu provést[111] s tím, že další případy zpracování, které (ne)vyžadují posouzení vlivu, může v budoucnu stanovit ÚOOÚ (čl. 35 odst. 4 a 5). K výkladu poměrně vágního pojmu „vysoké riziko“ vydala Pracovní skupina stanovisko, v němž uvádí deset zásadních kritérií, která je třeba v této souvislosti posuzovat.[112] Čím více těchto kritérií přitom správce splní, tím spíše bude jím prováděné zpracování osobních údajů představovat vysoké riziko pro práva a svobody fyzických osob. Pracovní skupina dochází k závěru, že pokud zaměstnavatel hodlá zavést monitoring zaměstnanců (včetně monitoringu prostor na pracovišti, aktivit zaměstnanců na internetu, pracovní výkonnosti, apod.), je povinen posouzení jeho vlivu

---

[111] Jde o následující případy: „*a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad; b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo c) rozsáhlé systematické monitorování veřejně přístupných prostorů.*“

[112] Tato kritéria zpravidla vyplývají z recitálů GDPR a patří mezi ně např. hodnocení subjektu údajů na základě zpracovaných osobních údajů, automatizované rozhodování o subjektu údajů s právními nebo jinými následky, systematičnost zpracování, zpracování citlivých údajů, zpracování osobních údajů ve velkém rozsahu, zpracování údajů zranitelných subjektů údajů, předávání osobních údajů mimo Evropskou unii, atd. Viz Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Výkladové stanovisko k posouzení vlivu na ochranu osobních údajů a určení, zda je pravděpodobné, že zpracování bude mít za následek vysoké riziko, pro účely Nařízení 2016/679 (v originále: „*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679"*) ze dne 4. dubna 2017, s. 8 – 9.

na ochranu osobních údajů provést vždy. Hlavním důvodem pro tento závěr je dle Pracovní skupiny splnění dvou zásadních kritérií, a to kritérium systematičnosti takového zpracování a kritérium zranitelnosti subjektu údajů z důvodu slabší pozice zaměstnance vůči zaměstnavateli.[113]

GDPR dále v čl. 35 odst. 9 požaduje, aby správce ve vhodných případech získal k zamýšlenému zpracování stanovisko subjektů údajů nebo jejich zástupců. Jak dovozuje Pracovní skupina, měl by zaměstnavatel s ohledem na toto pravidlo znát před zavedením monitoringu zaměstnanců stanovisko zástupců zaměstnanců, tj. rady zaměstnanců a/nebo odborových organizací působících u zaměstnavatele. Pokud zaměstnavatel monitoring zavede i přes negativní postoj zástupců zaměstnanců, měl by své důvody řádně zdokumentovat; jestliže se zaměstnavatel rozhodne je vůbec předem nekonzultovat (v případě, kdy se domnívá, že tato konzultace není na místě), měl by takový postup řádně zdůvodnit.[114] Nesplnění této povinnosti nicméně není nijak sankcionováno. Požadavek konzultace s odborovými organizacemi zřejmě vychází z nezávazného Kodexu ochrany osobních údajů zaměstnanců vydaného Mezinárodní organizací práce, kde je formulován v čl. 12.2 písm. b).[115]

Povinnost provést posouzení vlivu se vztahuje na zpracování osobních údajů zahájená až po účinnosti GDPR; Pracovní skupina však důrazně doporučuje, aby správci posouzení provedli dodatečně i pro dříve zahájená zpracování a aby je pravidelně aktualizovali minimálně každé tři roky (s ohledem na povahu zpracování, změny zavedených operací apod. může být nicméně nezbytné posouzení aktualizovat dříve).[116]

Posouzení musí dle čl. 35 odst. 7 GDPR zahrnovat alespoň a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce; b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska

---

[113] Tamtéž, 9 – 10.

[114] Tamtéž, s. 13.

[115] MEZINÁRODNÍ ORGANIZACE PRÁCE: *Kodex ochrany osobních údajů zaměstnanců* (v originále: „*Protection of Worker's Personal Data*“). 1. vydání. Ženeva: International Labour Office, 1997, 24 s. ISBN 92-2-110329-3.

[116] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Výkladové stanovisko k posouzení vlivu na ochranu osobních údajů a určení, zda je pravděpodobné, že zpracování bude mít za následek vysoké riziko, pro účely Nařízení 2016/679 (v originále: „*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679"*) ze dne 4. dubna 2017, s. 11 – 12.

účelů; c) posouzení rizik pro práva a svobody subjektů údajů; a d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s GDPR, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob. Při posouzení se má zohlednit též dodržování schválených kodexů chování. V reakci na GDPR vyšla pro oblast posouzení vlivu též nová technická norma (ISO/IEC 29134:2017 z června 2017).

Pokud z posouzení vlivu vyplyne, že zpracování osobních údajů může mít za následek vysoké riziko pro práva a svobody subjektů údajů, které nelze minimalizovat vhodnými technicko-organizačními opatřeními (zejména s ohledem na dostupné technologie nebo náklady na zavedení opatření), bude správce dle čl. 36 odst. 1 GDPR povinen před zahájením zpracování konzultovat ÚOOÚ. Pracovní skupina se opět snaží tuto problematiku vyjasnit; uvádí však pouze, že předchozí konzultace bude nezbytná v případě, kdy bude i po zavedení všech vhodných opatření stále hrozit nepřijatelné riziko, např. kdy budou subjektům údajů hrozit závažné nebo neodvratitelné následky, kterým se nelze vyhnout ani pomocí přijatých technicko-organizačních opatření, nebo kdy bude zřejmé, že se hrozící riziko skutečně naplní.[117]

GDPR dále požaduje, aby správce osobních údajů v určitých případech jmenoval pověřence pro ochranu osobních údajů. Jeho úkoly vymezuje čl. 39 GDPR a patří mezi ně především poskytování podpory správci a poradenská činnost v oblasti zpracování osobních údajů, dohled nad souladem zpracování s GDPR a dalšími příslušnými právními předpisy a spolupráce s dozorovým úřadem (ÚOOÚ). Pověřenec se též vyjadřuje k prováděnému posouzení vlivu na ochranu osobních údajů. Pověřenec může být jmenován jak z řad zaměstnanců správce, tak z externích odborníků; pak je činný na základě smlouvy o poskytování služeb (čl. 37 odst. 6 GDPR). Pro svou funkci musí splňovat dostatečné profesní záruky, především mít odborné znalosti práva a praktické zkušenosti v oblasti ochrany osobních údajů. Správce je povinen pověřenci poskytovat veškerou potřebnou součinnost a plně respektovat jeho nezávislost. Za plnění jeho úkolů jej nesmí jakkoli penalizovat; jestliže je pověřenec jeho zaměstnancem, nesmí s ním v této souvislosti ani rozvázat pracovní poměr. GDPR tak de facto vytváří novou

[117] Tamtéž, s. 18.

chráněnou kategorii zaměstnanců. I přes jmenování pověřence nicméně veškerá odpovědnost za zpracování osobních údajů v souladu s GDPR leží na správci.

Dle čl. 37 odst. 1 GDPR je jmenování pověřence povinné, pokud a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí; b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů (dle čl. 9 GDPR) a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů (dle čl. 10 GDPR).

Na základě výše uvedeného znění GDPR tak lze usoudit, že na soukromoprávní zaměstnavatele se v kontextu monitoringu zaměstnanců povinnost jmenovat pověřence vztahovat nebude; sledování zaměstnanců bude představovat pouze jejich podpůrnou, a nikoli hlavní (podnikatelskou) činnost. Nic však samozřejmě nebrání tomu, aby tito zaměstnavatelé pověřence jmenovali dobrovolně; v takovém případě se ale budou muset řídit příslušnými ustanoveními GDPR.

Naopak veřejnoprávní zaměstnavatelé budou povinni pověřence jmenovat za účelem jakéhokoli zpracování, tj. včetně monitoringu zaměstnanců (při němž dochází ke zpracování osobních údajů).[118] Jak uvádí Pracovní skupina, GDPR nedefinuje pojem orgánu veřejné moci či veřejného subjektu, a proto je třeba jej vykládat v souladu s příslušnou národní právní úpravou. Mezi veřejné subjekty (správní orgány) přitom na úrovni českého práva patří dle § 1 odst. 1 SŘ též právnické a fyzické osoby založené dle soukromého práva, které vykonávají působnost v oblasti veřejné správy (tyto subjekty nicméně nepatří mezi zaměstnavatele dle § 109 odst. 3 ZP[119]). Pracovní skupina proto v rámci dobré praxe doporučuje, aby i tito zaměstnavatelé pověřence jmenovali, a to pro

[118] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Příloha k Výkladovému stanovisku k pověřencům pro ochranu osobních údajů (v originále: „*Guidelines on Data Protection Officers (DPOs)"*) ze dne 13. prosince 2016 – Často kladené otázky (v originále „*Frequently Asked Questions*"), s. 1.

[119] Těmi jsou stát, územní samosprávný celek, státní fond, příspěvková organizace, jejíž náklady na platy a odměny za pracovní pohotovost jsou plně zabezpečovány z příspěvku na provoz poskytovaného z rozpočtu zřizovatele nebo z úhrad podle zvláštních právních předpisů, školská právnická osoba zřízená Ministerstvem školství, mládeže a tělovýchovy, krajem, obcí nebo dobrovolným svazkem obcí podle školského zákona, regionální rada regionu soudržnosti.

všechny případy zpracování, včetně zpracování osobních údajů zaměstnanců (tj. bez omezení na oblast výkonu působnosti v oblasti veřejné správy).[120] Změnu v této oblasti však ještě může přinést nová česká právní úprava, jež bude v souvislosti s GDPR přijata, neboť dle čl. 37 odst. 4 GDPR mohou být další případy povinného jmenování pověřence pro ochranu osobních údajů stanoveny vnitrostátním předpisem.

Další povinností zaměstnavatele jako správce osobních údajů po účinnosti GDPR bude vedení záznamů o činnostech zpracování dle čl. 30 GDPR. Záznamy musejí obsahovat vymezené údaje[121] a musejí být vedeny písemně, přičemž se počítá i elektronická forma. Řádné vedení záznamů bude klíčové pro doložení souladu zpracování s GDPR v případě kontroly ze strany ÚOOÚ; ten je oprávněn požadovat jejich zpřístupnění. GDPR sice od povinnosti vést záznamy osvobozuje zaměstnavatele s méně než 250 zaměstnanci, ovšem tato výjimka se dle čl. 30 odst. 5 GDPR nevztahuje na zaměstnavatele, kteří provádějí zpracování představující riziko pro práva a svobody subjektů údajů, systematické zpracování nebo zpracování citlivých údajů. Zaměstnavatelé, kteří provádějí monitoring svých zaměstnanců (jenž není pouze příležitostný a v jehož případě zpravidla lze konstatovat, že představuje riziko pro práva a svobody zaměstnanců), by proto měli vést záznamy o činnostech zpracování i přesto, že mají méně než 250 zaměstnanců. Motivací by jim mělo být zřejmě též lepší postavení vůči ÚOOÚ při případné kontrole (pochopitelně pouze v případě, že budou záznamy vedeny řádně).

Z výše uvedeného výkladu vyplývá, že zpracování osobních údajů po účinnosti GDPR bude ve srovnání se současným stavem pro zaměstnavatele jako správce znamenat vyšší míru odpovědnosti, zvýšené náklady i podstatnou administrativní zátěž. Zejména menší

---

[120] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Výkladové stanovisko k pověřencům pro ochranu osobních údajů (v originále: „*Guidelines on Data Protection Officers (DPOs)"*) ze dne 13. prosince 2016, s. 5 – 6.

[121] Dle čl. 30 odst. 1 musí obsahovat „*a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů; b) účely zpracování; c) popis kategorií subjektů údajů a kategorií osobních údajů; d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích; e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk; f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů; g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1*."

zaměstnavatelé by proto měli zvážit, zda jim monitoring zaměstnanců (se zpracováním osobních údajů) bude i za tuto cenu stát.

(h) Oznamovací povinnost vůči ÚOOÚ

Do účinnosti GDPR je zaměstnavatel jako správce osobních údajů v případě soustavného monitoringu se zpracováním osobních údajů povinen dle § 16 odst. 1 ZOOÚ takové zpracování oznámit ÚOOÚ prostřednictvím předepsaného formuláře. Oznámení musí obsahovat vymezené náležitosti a musí být provedeno ještě před zahájením monitoringu. Pokud do 30 dnů od doručení oznámení nezahájí ÚOOÚ řízení z důvodu možného porušení ZOOÚ (dle § 17 ZOOÚ), je zaměstnavatel po uplynutí této lhůty oprávněn monitoring zahájit a ÚOOÚ provede odpovídající zápis do registru zpracování osobních údajů. Jedná-li se o zpracování osobních údajů v rámci nahodilé kontroly zaměstnanců (např. s ohledem na dodržování zákazu užívání výrobních a pracovních prostředků zaměstnavatele pro soukromou potřebu zaměstnanců dle § 316 odst. 1 ZP), pak samozřejmě není zaměstnavatel povinen takové zpracování ÚOOÚ oznamovat; uplatní se výjimka dle § 18 odst. 1 písm. b) ZOOÚ, neboť půjde o zpracování potřebné pro uplatnění práv zaměstnavatele dle ZP.

Nový přístup ovšem v této oblasti razí GDPR, které dosavadní praxi oznamování zpracování považuje za administrativní a finanční zátěž, která však nepřispěla ve všech případech ke zlepšení ochrany osobních údajů. Tato obecná povinnost zatěžující všechny správce bez výjimky by proto měla být zrušena a nahrazena účinnějšími postupy, které by se zaměřily na taková zpracování, jež představují vysoké riziko pro práva a svobody fyzických osob (recitál 89 GDPR). Mezi tyto účinnější postupy patří zejména proces posouzení vlivu na ochranu osobních údajů s případnou povinností předchozí konzultace s ÚOOÚ a do jisté míry též vedení záznamů o činnostech zpracování (výklad k obojímu viz výše pod bodem (g)).

S novou právní úpravou, jež by měla být v souvislosti s účinností GDPR na úrovni českého práva přijata, proto bude oznamovací povinnost vůči ÚOOÚ v plném rozsahu zrušena.[122]

[122] ÚOOÚ: Obecné nařízení o ochraně osobních údajů v otázkách a odpovědích [online]. Publikováno dne 25. května 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-v-otazkach-a-odpovedich/d-23790/p1=3938>.

2. Metody monitoringu zaměstnanců

V této části práce se budu podrobněji věnovat jednotlivým typům kontrolních opatření, která zaměstnavatelé za účelem monitoringu svých zaměstnanců zavádějí nejčastěji. Tato kapitola pojednává zásadně pouze o způsobech soustavného monitoringu ve smyslu ustanovení § 316 odst. 2 ZP. Rovněž je třeba ji číst v kontextu předchozí kapitoly 1, kde jsou uvedeny parametry, jež musí zaměstnavatel splnit, aby byl jím zavedený monitoring oprávněný. Případné odchylky nebo doplnění s ohledem na konkrétní typ monitoringu, jakož i relevantní případy z rozhodovací praxe, nicméně pro přehlednost uvádím přímo v této kapitole.

2.1 Kontrola elektronické pošty

2.1.1 Úvodní poznámky; problematika listovního tajemství

Jedním z nejčastějších způsobů monitoringu zaměstnanců, kteří vykonávají převážnou část svých pracovních úkolů pomocí počítače, je kontrola elektronické pošty. Předně je třeba konstatovat, že elektronickou poštu zaměstnanců chrání listovní tajemství, které garantuje čl. 13 Listiny základních práv a svobod[123] a samozřejmě též řada mezinárodních smluv.[124] Též písemnosti zachycené v elektronické podobě (se zachycením obsahu právního jednání a určením jednající osoby) se dle § 562 odst. 1 OZ považují za dokumenty pořízené v písemné formě, tj. zaslouží si stejnou ochranu jako běžná písemná korespondence. Ostatně jak dlouhodobě konstatuje Pracovní skupina, soukromí zaměstnance by mělo být chráněno bez ohledu na skutečnost, zda pracuje online nebo offline, tj. jeho e-maily mají požívat stejné ochrany jako tradiční dopisy.[125] Neoprávněné narušení elektronické pošty navíc může naplnit základní skutkovou podstatu trestného činu porušení tajemství dopravovaných zpráv dle § 182 TZ

[123] Znění čl. 13 Listiny základních práv a svobod je následující: „*Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením*."

[124] Např. již zmiňovaný čl. 8 Úmluvy o ochraně lidských práv, čl. 17 Mezinárodního paktu o občanských a politických právech a čl. 12 Všeobecné deklarace lidských práv.

[125] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Pracovní dokument o sledování elektronických komunikací na pracovišti (v originále: „*Working document on the surveillance of electronic communications in the workplace"*) ze dne 29. května 2002, s. 20.

(tj. úmyslné porušení tajemství datové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá).

Na druhou stranu, znovu citujme Ústavní soud: „*…právo na ochranu před neoprávněnými zásahy do soukromí se zpravidla vztahuje na případy zásahů do soukromé a rodinné sféry, v nichž jednotlivec projevuje svou osobnost svobodně a autonomně. V této sféře se však neocitá za situace, kdy v prostředí zaměstnavatele vystupuje a plní funkce pracovního charakteru. Rovněž pak listovní tajemství, tajemství jiných písemností a záznamů, tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením, nelze vztahovat na činnost, která má být svou povahou činností pracovní*.“[126] Při splnění testu proporcionality (viz podrobněji kapitolu 1.3 výše) proto zaměstnavatel bude moci právo zaměstnance na ochranu listovního tajemství do jisté míry omezit ve prospěch svých vlastních práv.

Dle stanoviska ÚOOÚ je třeba v kontextu sledování elektronické pošty rozlišovat název e-mailové schránky, kterou příslušný zaměstnanec používá. Přestože e-mailovou schránku zaměstnanci zřídí zaměstnavatel, který také (zpravidla) vlastní příslušnou doménu, zní-li e-mailová adresa na jméno konkrétního zaměstnance (např. jan.novak@domena.com), má být veškerá pošta doručená na tuto adresu považována za soukromou elektronickou poštu tohoto zaměstnance. Jiná situace by nastala v případě, kdy by název e-mailové adresy zněl např. info@domena.cz, obchod@domena.cz, a podobně obecným způsobem. Taková schránka má být považována za tzv. úřední a nikoli soukromou, a to i v případě, kdy by byl její správou pověřen pouze jediný konkrétní zaměstnanec.[127] ÚOOÚ zřejmě vychází z předpokladu, že odesílatel v tomto případě nemůže rozumně očekávat, že se jeho zpráva odeslaná na takto obecnou adresu dostane k rukám konkrétní osoby.

S takovým výkladem část literatury ne zcela souhlasí; pokud je e-mailová schránka zřízena zaměstnavatelem na pracovní počítačové stanici ve vlastnictví či užívání zaměstnavatele za účelem jejího využití při výkonu práce, pak ji zaměstnanec nemůže

[126] Usnesení Ústavního soudu sp. zn. I. ÚS 452/09 ze dne 31. března 2009.

[127] ÚOOÚ: Stanovisko č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště, s. 3. Únor 2009.

považovat za zcela soukromou. Skutečnost, že název schránky nese jméno zaměstnance, však logicky zvyšuje jeho míru očekávání (a též míru očekávání jeho kontaktů) ohledně zachovávání soukromí doručených zpráv.[128]

Dle Morávka může mít rozlišování soukromé a úřední adresy tak, jak je prezentoval ve svém výše uvedeném stanovisku ÚOOÚ, pouze jakýsi orientační význam s ohledem na identifikační znaky jednotlivých doručených/odeslaných zpráv (odesílatel, příjemce, případně oslovení adresáta) a k rozlišení povahy těchto zpráv.[129] S tímto názorem souhlasím; nelze *a priori* připustit výklad, že veškeré zprávy doručené na „úřední" e-mailovou adresu jsou pracovní, aniž by byl brán ohled na jejich obsah, a naopak, že veškeré zprávy doručené na „soukromou" adresu jsou soukromé povahy. Ze stanoviska ÚOOÚ přitom takový výklad vyplývá, když ÚOOÚ zásadně zakazuje sledování e-mailových zpráv doručených do „soukromé" e-mailové schránky (tj. nikoli úřední). Zaměstnavatel smí nejvýše sledovat pouze provoz takové schránky, tj. počet doručených a odeslaných e-mailů a hlavičky e-mailu včetně údaje o adresátovi/odesílateli. Otevřít a číst konkrétní zprávu může zaměstnavatel dle názoru ÚOOÚ pouze tehdy, je-li z údajů v hlavičce zřejmé, že se jedná o pracovní e-mail, který je třeba vyřídit místo příslušného zaměstnance, jenž na něj z objektivních důvodů (např. kvůli dlouhodobé nemoci) nebude moci odpovědět včas, a zaměstnavateli by proto hrozila újma na jeho právech.[130] V takovém případě nahodilého přístupu do elektronické schránky by se ani nejednalo o zpracování osobních údajů[131] (pro podrobnější výklad viz kapitolu 2.1.2(c) níže).

Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze jeho činnosti ve smyslu § 316 odst. 2 ZP, je oprávněn za splnění testu proporcionality a zásad monitoringu elektronickou poštu zaměstnance sledovat. Takovým závažným důvodem může být např. ochrana majetku zaměstnavatele, síťová bezpečnost, ochrana

---

[128] BĚLINA, Miroslav a kolektiv. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015, xviii, s. 1245. Velké komentáře. ISBN 978-80-7400-290-8.

[129] MORÁVEK, Jakub. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy.* 2017, roč. 25, č. 17, s. 580. ISSN 1210-6410.

[130] ÚOOÚ: Stanovisko č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště, s. 3 – 4. Únor 2009.

[131] BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi*. 2. vyd. Praha: LINDE, 2010, s. 145. ISBN 978-80-7201-817-8.

utajovaných skutečností, bankovního nebo obchodního tajemství, důvěrných informací nebo know-how a kontrola dodržování povinnosti mlčenlivosti ze strany zaměstnanců.

S přihlédnutím ke konkrétním okolnostem daným u zaměstnavatele pak bude záležet na tom, jaký způsob monitoringu bude ještě považován za legitimní a jaký už nikoli. Vždy je však třeba pamatovat na skutečnost, že e-maily soukromé povahy jsou chráněny listovním tajemstvím, ať už jsou doručeny na „úřední" či „soukromou" e-mailovou adresu, a zaměstnavatel není oprávněn je číst. Soukromý charakter zprávy by měl zaměstnavatel vyhodnotit na základě identifikačních znaků typu odesílatel, předmět či oslovení příjemce. Pokud vyhodnotí, že se jedná o pracovní komunikaci, avšak po otevření e-mailu se přesto ukáže, že jde o soukromou zprávu, je zaměstnavatel povinen čtení zprávy s ohledem na listovní tajemství okamžitě ukončit.[132]

2.1.2 Základní způsoby monitoringu elektronické pošty

Monitoring elektronické pošty lze provádět v zásadě dvěma základními způsoby, a to jako sledování provozu e-mailové schránky a jako sledování obsahu e-mailových zpráv. Sledování provozu e-mailové schránky spočívá ve sledování údajů o přijatých i odeslaných e-mailových zprávách včetně adres příjemců/odesílatelů, předmětu, data, času a velikosti přijatých/odeslaných zpráv a skutečnosti, zda ke zprávě byla připojena příloha či nikoli a v jakém formátu. Sledování provozu e-mailové schránky logicky představuje méně invazivní zásah do soukromí zaměstnance než sledování obsahu e-mailových zpráv, které zahrnuje vstup do zpráv jako takových. Zatímco v rámci sledování provozu schránky lze dle výkladu ÚOOÚ[133] sledovat i soukromou poštu, sledovat obsah zpráv lze pouze v případě pracovní korespondence. V kontextu monitoringu obsahu e-mailových zpráv Pracovní skupina připomíná povinnost zaměstnavatele brát ohled též na soukromí odesílatelů/příjemců zpráv zaměstnance, kteří jsou vůči zaměstnavateli logicky ve zcela odlišném postavení než jeho zaměstnanci, případně k němu nemají vůbec žádný vztah. Pracovní skupina nabízí

[132] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, dostupné elektronicky v systému ASPI. Část V., kapitola 2.1.2.2. ISBN 978-80-7478-139-1.

[133] ÚOOÚ: Stanovisko č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště, s. 3. Únor 2009.

řešení v podobě připojení automatického oznámení o zavedení sledovacích opatření na konec každého e-mailu, který zaměstnanec odesílá, aby adresáti zpráv byli na možný monitoring upozorněni[134]. Tímto způsobem však pochopitelně nebudou moci být informováni odesílatelé, kteří zaměstnance kontaktují jako první.

Dalším rozlišovacím prvkem co se způsobu monitoringu týče, je skutečnost, zda se jedná o soustavné nebo o časově omezené až nahodilé sledování. Zvolený způsob monitoringu by měl zaměstnavatel každopádně zakotvit ve vnitřním předpise, který by podrobně vymezoval důvody pro zavedení sledování elektronické pošty, rozsah sledování a způsob jeho výkonu.

(a) Nahodilé sledování provozu elektronické schránky

Nahodilé či časově omezené sledování provozu elektronické schránky bude prováděno nepravidelně jako namátková kontrola. Může jít o kontrolu ve smyslu § 316 odst. 1 ZP v případě, kdy zaměstnavatel výslovně nedovolí ani netoleruje užívání jím zřízené pracovní elektronické schránky pro soukromé účely zaměstnance. Pokud však zaměstnavatel současně nesplní podmínku závažného důvodu spočívajícího ve zvláštní povaze své činnosti (viz kapitolu 1.4), bude muset být taková kontrola skutečně pouze namátková, respektive zaměstnavatel musí být schopen obhájit, že je vykonávána přiměřeným způsobem. Pokud by k takové kontrole docházelo příliš často (bez odůvodněného podezření zaměstnance ze zneužívání pracovních prostředků zaměstnavatele), pak by zřejmě přiměřená nebyla, a tudíž by byla nezákonná.

Nahodilým sledováním provozu elektronické schránky může zaměstnavatel rovněž zkontrolovat, zda zaměstnanec řádně vykonává svou práci, odpovídá včas na e-maily zákazníků a dalších osob, s nimiž má v zájmu zaměstnavatele komunikovat (např. jiná oddělení a/nebo pracoviště zaměstnavatele a orgány státní správy), případně zda zaměstnanec dodržuje své další povinnosti. Typicky může jít o poměrně často ukládanou povinnost přeposílat veškeré příchozí pracovní e-maily svému nadřízenému zaměstnanci či přímo zaměstnavateli a rovněž jim všechny odchozí pracovní e-maily odesílat v kopii. Pro tento typ kontroly musí zaměstnavatel splnit podmínky stanovené

[134] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Pracovní dokument o sledování elektronických komunikací na pracovišti (v originále: „*Working document on the surveillance of electronic communications in the workplace*“) ze dne 29. května 2002, s. 17 – 18.

v § 316 odst. 2 ZP a je rovněž povinen o této kontrole informovat zaměstnance ve smyslu § 316 odst. 3 ZP.

V případě tohoto typu sledování zpravidla nepůjde o zpracování osobních údajů zaměstnance; zaměstnavatel pouze jednou za čas zkontroluje identifikační znaky e-mailových zpráv. Nevyvodí-li z kontroly žádná pochybení na straně zaměstnance, zpravidla nebude mít potřebu zjištěné údaje zaznamenávat či jinak zpracovávat. V opačném případě by se samozřejmě o zpracování osobních údajů jednalo a zaměstnavatel by byl povinen dodržovat povinnosti vyplývající ze ZOOÚ a GDPR uvedené v kapitole 1.5.2 výše.

(b) Soustavné sledování provozu elektronické schránky

Soustavným sledováním je myšleno dlouhodobé až nepřetržité a trvalé sledování identifikačních znaků příchozích a odchozích e-mailových zpráv. V porovnání s nahodilým sledováním provozu schránky by měl mít zaměstnavatel pro soustavný monitoring pádnější důvod, aby mohl zdůvodnit, proč k ochraně jeho práv nestačí méně invazivní nahodilé sledování. Takovým konkrétním důvodem může být např. časté zneužívání pracovních prostředků zaměstnavatele k soukromým účelům zaměstnanců, kontrola dodržování zákazu komunikace s konkurenčními společnostmi, ochrana know-how, obchodního tajemství a nehmotného majetku, apod.

Soustavné sledování provozu elektronické schránky bude v každém případě představovat zpracování osobních údajů. Pro jeho zavedení také zaměstnavatel musí splnit podmínky stanovené v § 316 odst. 2 ZP.

(c) Nahodilé sledování obsahu e-mailových zpráv

Kontrola obsahu jednotlivých e-mailových zpráv již představuje poměrně významný zásah do soukromí zaměstnance, a zaměstnavatel by ji proto měl velmi pečlivě odůvodnit. Ke sledování obsahu e-mailových zpráv bude zaměstnavatel oprávněn sáhnout teprve v případě, že pro ochranu jeho práv nebude postačovat kontrola provozu e-mailové schránky (ať už nahodilá či soustavná). Takovým případem může být situace, kdy je zaměstnanec dlouhodobě nepřítomen v práci a není dosažitelný (tj. nemůže zprávu sám přeposlat přímo zaměstnavateli nebo jinému zaměstnanci) a zaměstnavatel potřebuje pro ochranu svých zájmů zamezit prodlení ve vyřizování pracovní

komunikace (např. z důvodu hrozícího nebezpečí propadnutí lhůty při účasti ve výběrovém řízení ohledně významné zakázky nebo při komunikaci s orgány státní správy). Dalším důvodem pro nahodilý vstup zaměstnavatele do e-mailových zpráv zaměstnance může být důvodné podezření jeho osoby z páchání trestné činnosti nebo z poškozování zaměstnavatele (např. vynášení know-how a obchodního tajemství, přeposílání důvěrných informací konkurenci, apod.). Znovu připomeňme, že zaměstnavatel je oprávněn otevřít a číst pouze komunikaci pracovního charakteru.

Jako v případě nahodilého sledování provozu elektronické schránky ani v rámci tohoto způsobu monitoringu zpravidla nebude docházet ke zpracování osobních údajů zaměstnance (uplatní se obdobný výklad jako ten uvedený výše pod bodem (a)).

(d) Soustavné sledování obsahu e-mailových zpráv

Soustavný monitoring obsahu e-mailových zpráv představuje jeden z nejvýraznějších zásahů do soukromí zaměstnance, k jakému může na pracovišti vůbec docházet. S ohledem na princip proporcionality si lze jen velmi obtížně představit situace, za nichž by zaměstnavatel byl schopen obhájit soustavné sledování obsahu veškerých odeslaných a doručených pracovních e-mailů zaměstnance a dostatečně zdůvodnit, proč jeho zájmy nemohou ochránit méně invazivní kontrolní mechanismy.[135] Přípustnější variantou tohoto typu monitoringu by mohlo být nastavení určitých omezujících kritérií, např. sledování obsahu pouze některých pracovních e-mailů vytipovaných podle předem určených klíčových slov, podle toho, zda je k nim připojena příloha (případně v jakém formátu), nebo podle typu odesílatele/příjemce zpráv (např. konkurenční společnosti, konkrétně vymezení důležití zákazníci, apod.). Přesto by i pro tento relativně omezený soustavný monitoring měl mít zaměstnavatel velmi silný důvod, např. ochranu bankovního či obchodního tajemství, kontrolu dodržování povinnosti mlčenlivosti, ochranu velmi cenného a těžko dostupného know-how apod. Mělo by se přitom jednat o situaci, kdy by zaměstnavateli mohla být v důsledku zacházení zaměstnance s elektronickou poštou způsobena závažná újma, jejíž hrozbu nelze odvrátit méně invazivními prostředky; např. proto, že tyto méně invazivní prostředky již v minulosti

[135] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „Opinion 2/2017 on data processing at work“) ze dne 8. června 2017, s. 13.

selhaly, a zaměstnavatel v důsledku zneužití elektronické schránky ze strany svého zaměstnance utrpěl závažnou újmu.

Tento typ monitoringu bude pochopitelně představovat zpracování osobních údajů. S ohledem na velmi významný dopad tohoto typu sledování pro práva a svobody zaměstnanců by měl zaměstnavatel jeho zavedení předem konzultovat s ÚOOÚ; s účinností GDPR tak bude zřejmě i povinen učinit, a to podle čl. 36 odst. 1 GDPR (podrobněji viz kapitolu 1.5.2(g)).

2.1.3 Konkrétní příklady scénářů monitoringu elektronické pošty

V této podkapitole uvedu několik příkladů, jakým způsobem je možné sledování elektronické pošty nastavit v praxi. Předně by však měl zaměstnavatel vyřešit otázku, jaká pravidla nastavit ohledně soukromých e-mailových zpráv, k jejichž výskytu v elektronické schránce zaměstnance může chtě nechtě dojít. To je nutné zejména v případě zamýšleného sledování obsahu e-mailových zpráv za účelem minimalizace rizika, že zaměstnavatel nesprávně vyhodnotí identifikační znaky zprávy a neoprávněně otevře soukromý e-mail, čímž poruší listovní tajemství zaměstnance. I když se zaměstnavatel bude držet základního nastavení vyplývajícího z § 316 odst. 1 ZP, tj. zaměstnanci výslovně nedovolí používat elektronickou schránku pro soukromou potřebu, nemůže zabránit tomu, aby zaměstnance na jeho pracovní e-mailové adrese kontaktovaly jiné osoby v soukromém módu. Doručení soukromé e-mailové zprávy přes zákaz stanovený § 316 odst. 1 ZP nemůže samo o sobě představovat porušení povinnosti zaměstnance tento zákaz dodržovat, ledaže zaměstnanec takovou situaci bez souhlasu zaměstnavatele zaviněně vyvolal a tím zaměstnavatele zatížil.[136]

Řada zaměstnavatelů zpravidla mlčky toleruje soukromou komunikaci zaměstnanců prostřednictvím pracovní e-mailové schránky, pokud nepřesáhne určitou únosnou míru a nemá viditelný dopad na jejich pracovní výkonnost, aniž by však v této souvislosti nastavili jasná pravidla chování. Pak ovšem nebudou oprávněni za takovou činnost postihnout např. pouze vybraného zaměstnance, a to s ohledem na zásadu rovného

[136] MORÁVEK, Jakub. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy.* 2017, roč. 25, č. 17, s. 580. ISSN 1210-6410.

zacházení. Vhodnějším řešením proto v takovém případě je předem stanovit konkrétní zásady užívání elektronické schránky v omezené míře též pro soukromé účely ve vnitřním předpise a dodržování těchto zásad přiměřeně, avšak pravidelně, kontrolovat. Zaměstnavatel např. může požadovat, aby zaměstnanci soukromou komunikaci četli a vyřizovali mimo pracovní dobu[137], případně aby veškerou přijatou soukromou komunikaci ještě během téhož dne či do několika hodin od jejího doručení vymazali nebo uložili do zvláštní složky označené jako „soukromá". Může též zaměstnancům zakázat komunikovat vzájemně mezi sebou v soukromém módu prostřednictvím elektronické schránky s tím, že jim umožní používat pro tyto účely interní chatovací aplikaci s případně nastaveným každodenním, týdenním či měsíčním časovým omezením jejího užívání.

Obdobný výklad platí i pro další funkce, jež zpravidla současné elektronické schránky umožňují, např. pro kalendář, upomínky a poznámky. Pokud je zaměstnavatelem umožněno či tolerováno jejich užívání též pro soukromé účely, měli by mít zaměstnanci možnost určité položky označit jako „soukromé" a tím znemožnit jejich zobrazení zaměstnavateli.[138]

(a) „Nouzový" přístup do elektronické schránky

Může dojít k situaci, kdy zaměstnanci bude doručen důležitý pracovní e-mail, avšak tento zaměstnanec nebude dostupný a objektivně schopný jej pro svou nepřítomnost sám včas vyřídit, v důsledku čehož bude zaměstnavateli hrozit vznik újmy. Pro tyto případy může zaměstnavatel nastavit monitoring provozu elektronické schránky (omezený časově po dobu nepřítomnosti zaměstnance) a současně monitoring obsahu konkrétních e-mailových zpráv identifikovaných v rámci monitoringu provozu schránky, jejichž včasné vyřízení je nezbytně nutné pro ochranu zájmů zaměstnavatele. Zaměstnavatel musí pro tento scénář splnit podmínky § 316 odst. 2 a 3 ZP, jinak by

[137] BĚLINA, Miroslav a kolektiv. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015, xviii, s. 1245. Velké komentáře. ISBN 978-80-7400-290-8.

[138] Viz např. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*") ze dne 8. června 2017, s. 15.

jednal v rozporu se zákonem.[139] Nebude se však jednat o zpracování osobních údajů nepřítomného zaměstnance.

Ve vnitřním předpise by měl zaměstnavatel konkretizovat situace, kdy bude aplikován monitoring provozu elektronické schránky, tj. nepřítomnost zaměstnance na pracovišti (pochopitelně z jiného důvodu než kvůli práci mimo pracoviště zaměstnavatele) v rozsahu převyšujícím konkrétně stanovený počet dnů. Čím nižší počet dnů bude takto určen, tím větší zásah do soukromí bude monitoring představovat. Zaměstnavatel v tomto směru musí zohlednit pravděpodobnost vzniku újmy v důsledku opožděného vyřízení pracovní komunikace s tím, že v úvahu je třeba vzít pracovní zařazení jednotlivých zaměstnanců. Jiný počet dnů pro zahájení sledování provozu schránky bude akceptovatelný např. u zaměstnanců dodavatele zboží podléhajícího rychlé zkáze, kteří mají na starost komunikaci se zákazníky, či u vedoucího právního oddělení (např. tři dny) než v případě zaměstnanců pracujících na oddělení reklamací se lhůtou pro jejich vyřízení v délce 30 dnů (např. dva týdny).

Současně může zaměstnavatel trvat na povinnosti nastavit v elektronické poště automatickou odpověď informující odesílatele zpráv o nepřítomnosti zaměstnance s uvedením kontaktu na jeho zástupce, což bude možné v případě plánované nepřítomnosti zaměstnance. Pro případ neplánované nepřítomnosti zaměstnance na pracovišti (případně pro případ, kdy zaměstnanec opomene nastavit automatickou odpověď sám) může zaměstnavatel ve vnitřním předpise určit, že tuto automatickou odpověď zaměstnanci nastaví k tomu pověřený zaměstnanec (např. přímo nadřízený zaměstnanec, asistentka, pracovník oddělení lidských zdrojů apod.).

Dále by měl zaměstnavatel ve vnitřním předpise identifikovat okolnosti, za nichž bude moci otevřít a vyřídit pracovní e-mailové zprávy místo zaměstnance v době jeho nepřítomnosti. Může jít o situace, kdy (i) není v elektronické schránce včas nastavena automatická odpověď a zaměstnanci je doručena zpráva, jejíž vyřízení je nezbytně nutné, nebo (ii) sice je včas nastavena automatická odpověď, avšak odesílatel uvedeného zástupce zaměstnance přesto nekontaktuje, jeho zprávu ovšem musí zaměstnavatel pro ochranu svých zájmů včas vyřídit. Ve vnitřním předpise by

[139] JOUZA, Ladislav. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. *Bulletin advokacie*. 2014, č. 6, s. 29. ISSN 1210-6348.

zaměstnavatel též měl určit zaměstnance, kteří budou oprávněni provoz elektronické schránky nepřítomného zaměstnance sledovat a také otevřít a vyřídit příslušné e-mailové zprávy. Vnitřní předpis může též oprávnit zaměstnance, aby si takového svého „zástupce“ (případně alternativně dva zástupce pro jejich vzájemnou zastupitelnost) vybral sám.

(b) Soustavné sledování provozu e-mailových zpráv s výhradou čtení jejich obsahu

Řekněme, že zaměstnavatel je povinnou osobou dle § 2 AML Zákona, např. bankou či platební institucí. Je tudíž povinen dle § 21 odst. 1 AML Zákona zavést a uplatňovat odpovídající strategie a postupy vnitřní kontroly a komunikace ke zmírňování a účinnému řízení rizik legalizace výnosů z trestné činnosti a financování terorismu, jakož i k plnění dalších povinností stanovených AML Zákonem. Za tímto účelem se rozhodne zavést soustavný monitoring provozu e-mailových zpráv zaměstnanců, kteří mohou přijít do styku s osobami, jež by mohly mít v úmyslu uzavírat se zaměstnavatelem podezřelé obchody ve smyslu AML Zákona, např. s osobami, vůči nimž Česká republika uplatňuje mezinárodní sankce podle zvláštního zákona. Tyto důvody pro zavedení soustavného monitoringu provozu e-mailových zpráv (jež budou představovat závažný důvod ve smyslu § 316 odst. 2 ZP) zaměstnavatel uvede ve vnitřním předpise spolu s povinnostmi zaměstnanců vyplývajících z AML Zákona a dalších souvisejících právních předpisů. Zaměstnavatel rovněž ve vnitřním předpise specifikuje podmínky, za nichž bude moci otevřít pracovní e-mailovou zprávu doručenou zaměstnanci, kterou identifikuje jako podezřelou ve smyslu AML Zákona. Může jít o případy, kdy bude odesílatelem či adresátem zprávy přímo podezřelá osoba nebo osoba ze státu, na nějž se vztahují mezinárodní sankce, případně zaměstnanci a jiní zástupci těchto osob. Skutečnost, že se může jednat o podezřelou zprávu, respektive o podezřelého adresáta či odesílatele zprávy, zaměstnavatel vyhodnotí na základě identifikačních znaků příslušných zpráv. Ve vnitřním předpise by měl zaměstnavatel též určit, co se bude dít v případě, že se bude skutečně jednat o podezřelou zprávu.

Prováděním monitoringu bude pověřeno zvláštní oddělení zaměstnavatele (např. oddělení řízení rizik). Protože se bude jednat o zpracování osobních údajů, musí zaměstnavatel řádně splnit podmínky vyplývající ze ZOOÚ a GDPR.

(c) Sledování obsahu e-mailových zpráv podle klíčových slov

V tomto scénáři mějme zaměstnavatele, který je významným soutěžitelem na trhu např. ve stavebním průmyslu. Protože již v minulosti byl účastníkem řízení vedeného proti němu pro porušení předpisů v oblasti ochrany hospodářské soutěže a zároveň se obává, že v jeho oboru může často docházet ke korupčnímu jednání, rozhodl se zaměstnavatel pro striktní dohled nad zaměstnanci za účelem zamezení podobnému nežádoucímu chování, za něž by jemu jako zaměstnavateli mohla být přičítána odpovědnost. Motivací mu je též liberační důvod dle § 8 odst. 5 TOPO, podle něhož se může právnická osoba zprostit trestní odpovědnosti dle TOPO, pokud vynaložila veškeré úsilí, které na ní bylo možno spravedlivě požadovat, aby spáchání protiprávního činu svými zaměstnanci zabránila.

Zaměstnavatel zaměstnance ve vnitřním předpise informuje o striktním zákazu užívat pracovní elektronickou schránku k soukromým účelům dle § 316 odst. 1 ZP a s tím související povinnosti mazat veškeré příchozí soukromé e-mailové zprávy ihned po jejich otevření. Zároveň zavede podrobná pravidla ohledně povinnosti zaměstnanců předcházet korupci a porušování pravidel hospodářské soutěže (např. zákaz přijímání či dávání jakýchkoli darů, podmínky komunikace s ostatními soutěžiteli a s odběrateli, povinnost oznamovat podezření na jakékoli nekalé praktiky svému nadřízenému zaměstnanci, apod.). Před zahájením monitoringu jako takového nechá zaměstnavatel zaměstnance podepsat potvrzení o vymazání veškeré stávající soukromé komunikace z pracovní schránky. Následně zavede soustavný monitoring obsahu e-mailových zpráv, který bude omezen na klíčová slova indikující možnou korupci a/nebo chování v rozporu s pravidly hospodářské soutěže.

Pomocí automaticky nastaveného programu budou veškeré e-mailové zprávy odesílané zaměstnancem (spolu s připojenými přílohami) prohledány s ohledem na výskyt klíčových slov. Bude-li zachycena zpráva obsahující některé z klíčových slov nebo jejich kombinaci, bude odeslání zprávy pomocí programu automaticky zablokováno a zaměstnanec obdrží e-mailovou zprávu informující jej o skutečnosti nalezení klíčových slov a blokaci odeslání zprávy. Následně k tomu pověřený zaměstnanec prověří obsah e-mailové zprávy s ohledem na skutečné riziko korupčního chování či chování v rozporu s pravidly hospodářské soutěže. V případě planého poplachu bude

zachycená zpráva odeslána a veškeré údaje o předchozím zpracování osobních údajů zaměstnance vymazány; zároveň bude zaměstnanec o těchto skutečnostech informován. V případě, že z obsahu e-mailové zprávy bude vyplývat skutečnost, že zaměstnanec porušil své povinnosti v oblasti předcházení korupci a dodržování pravidel hospodářské soutěže, bude zaměstnavatel oprávněn přijmout odpovídající kroky v závislosti na závažnosti takového porušení.

Ke zmírnění rizik vyplývajících z tohoto způsobu monitoringu pro ochranu soukromí zaměstnance může zaměstnavatel umožnit zaměstnancům otestovat si jimi odesílanou e-mailovou zprávu na výskyt klíčových slov před jejím samotným odesláním. V takovém případě pak budou mít zaměstnanci na výběr zprávu neodeslat a vyhnout se tak podrobnějšímu prověřování e-mailové zprávy a případným negativním důsledkům z toho vyplývajícím. Tuto praxi doporučuje s ohledem na zásadu transparentnosti též Pracovní skupina.[140]

2.1.4 Relevantní rozhodovací praxe

(a) Evropský soud pro lidská práva

Problematice sledování elektronické pošty zaměstnance (respektive obdobné komunikace uskutečněné prostřednictvím online aplikace) se věnoval Evropský soud pro lidská práva ve věci Coplandová proti Spojenému království (rozsudek ze dne 3. dubna 2007) a ve věci Bărbulescu proti Rumunsku (rozsudek ze dne 12. ledna 2016). Případ pana Bărbulescu je podrobněji popsán v kapitole 1.4 výše, ale spíše než soustavného monitoringu soukromé komunikace se týkal kontroly dodržování zákazu užívání pracovních prostředků zaměstnavatele (konkrétně aplikace Yahoo! Messenger) pro soukromé účely. Převedeme-li tento případ na českou právní úpravu, týkal se § 316 odst. 1 ZP.

[140] Viz Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 15.

Soustavného sledování zaměstnanců (ve smyslu § 316 odst. 2 ZP) se týkal případ paní Coplandové. Zaměstnavatel skrytě[141] sledoval (kromě jiného) její elektronickou poštu, přičemž dle tvrzení zaměstnavatele toto sledování trvalo několik měsíců, dle tvrzení zaměstnankyně však nejméně po dobu šesti měsíců. Důvodem zavedení monitoringu byla kontrola skutečnosti, zda paní Coplandová nadměrně neužívá pracovní prostředky zaměstnavatele pro svou soukromou potřebu. Ačkoli v době sledování neexistoval žádný vnitřní předpis upravující možnost soukromého užívání pracovních prostředků zaměstnavatele, byla tato praxe ze strany zaměstnavatele fakticky tolerována. V rámci monitoringu elektronické pošty se zaměstnavatel zaměřil na analýzu odchozích e-mailových zpráv, tj. sledoval e-mailové adresy adresátů a dále datum a čas odeslání e-mailů ze schránky paní Coplandové. Z výsledků sledování nevyvodil zaměstnavatel žádné důsledky (paní Coplandová byla zaměstnána u stejného zaměstnavatele dokonce i v době podání stížnosti k soudu). O zavedení sledovacích opatření se tak paní Coplandová dozvěděla až s odstupem několika měsíců po ukončení monitoringu, a to od svých kolegů.

Evropský soud pro lidská práva v daném případě shledal porušení práva paní Coplandové na soukromí garantované v čl. 8 Úmluvy o ochraně lidských práv a základních svobod, a to z důvodu, že (i) sledování paní Coplandové probíhalo skrytě bez předchozího upozornění ze strany zaměstnavatele (přičemž paní Coplandová mohla vzhledem k toleranci soukromého užívání pracovních prostředků patřících zaměstnavateli legitimně očekávat, že její soukromí na pracovišti nebude narušováno), a (ii) v době monitoringu neexistovala ve Spojeném království právní úprava, jež by sledování zaměstnanců umožňovala, a dovolila tak aplikovat výjimku z čl. 8 Úmluvy o ochraně lidských práv a základních svobod.[142]

(b) ÚOOÚ a soudy České republiky

Veřejně dostupných rozhodnutí ÚOOÚ a českých soudů na téma monitoringu elektronické pošty není mnoho; uveďme však alespoň jeden případ, který ÚOOÚ

[141] K problematice skrytého sledování viz kapitolu 1.5.2(b) výše.

[142] Rozsudek Evropského soudu pro lidská práva, stížnost č. 62617/00, ze dne 3. dubna 2007, Věc Coplandová proti Spojenému království.

zmiňuje ve své výroční zprávě za rok 2010 v rámci poznatků inspektorů z kontrolní činnosti.

Šlo o situaci, kdy vysoká škola znepřístupnila e-mailovou schránku svému původnímu rektorovi poté, co byl jmenován nový rektor. E-mailová schránka, která byla zřízena pod jménem bývalého rektora (a zároveň bývalého zaměstnance), pak byla následně zpřístupněna novému vedení školy s odůvodněním, že se nejednalo o soukromou schránku, ale o schránku rektora z titulu jeho postavení v čele vysoké školy, a bylo proto třeba ověřovat, zda do této e-mailové schránky nebyla doručena pošta určená vysoké škole jako takové. Kontrola ze strany ÚOOÚ proběhla po devíti měsících od ukončení funkce bývalého rektora a jeho e-mailová schránka stále existovala. ÚOOÚ posoudil případ tak, že s ohledem na skutečnost, kdy bývalý rektor nepoužíval dvě různé e-mailové schránky, z nichž jedna by byla určena pro korespondenci s ním v postavení rektora vysoké školy a druhá pro korespondenci s ním jakožto učitelem nebo kolegou, ale pouze jednu, je třeba považovat veškerou korespondenci v této schránce za jeho osobní. Vysoká škola tak postupovala v rozporu se zákonem, když e-mailovou schránku svého bývalého zaměstnance bez jeho souhlasu neoprávněně prohlížela (v tomto případě by mohl být právním titulem ke zpracování osobních údajů právě pouze souhlas bývalého zaměstnance jako subjektu údajů). Řešením mělo být zrušení e-mailové schránky a nastavení automatické odpovědi s informací o ukončení funkce bývalého rektora a se sdělením názvu e-mailové adresy nového rektora.[143]

2.2 Kontrola činnosti zaměstnanců na internetu

2.2.1 Úvodní poznámky

Dalším z velmi častých způsobů monitoringu zaměstnanců pracujících převážně na počítači, který jim za účelem výkonu práce svěřil zaměstnavatel, patří kontrola jejich činnosti na internetu. Důvody, proč si zaměstnavatel přeje mít pod kontrolou užívání internetu na pracovišti, mohou být různé. Jako závažný důvod dle § 316 odst. 2 ZP pro účely sledování užívání internetu však dle mého názoru obstojí zajišťování síťové

[143] ÚOOÚ: Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2010. Brno: Masarykova univerzita, 2011, s. 27 – 28. ISBN 978-80-210-5428-8.

bezpečnosti zaměstnavatele, ochrany dat a řádného provozu systému, který by mohl být v důsledku velkého toku pro práci nepotřebných dat zahlcen, čímž by kromě jiného docházelo ke zpomalování práce ostatních zaměstnanců. Se síťovou bezpečností a ochranou dat ovšem souvisí též zájem zaměstnavatele zejména na ochraně jeho (nehmotného) majetku, obchodního tajemství a know-how, jakož i na dodržování povinnosti mlčenlivosti. V důsledku zaměstnancových aktivit na internetu by totiž mohlo dojít k zavirování počítače či zavlečení různých špionážních a podobně nežádoucích programů, pomocí nichž by mohly třetí osoby k těmto chráněným hodnotám a informacím neoprávněně získat přístup. Dalším důvodem jistě bude kontrola efektivního využívání pracovní doby ze strany zaměstnanců. Není možné, aby zaměstnanci trávili nezanedbatelnou část své pracovní doby surfováním na internetu, a proto nestíhali plnit své pracovní úkoly, které by pak případně museli dohánět v rámci práce přesčas. To by pro zaměstnavatele znamenalo zbytečné náklady.

V době paušálních plateb za internet vázaných na určité období by jako závažný důvod ve smyslu § 316 odst. 2 ZP dle mého názoru neobstála ochrana majetku zaměstnavatele ve smyslu nákladů na připojení k internetu. Výjimkou by mohla být situace, kdy by zaměstnavatel neměl v daném místě pokrytí internetem možnost mít k dispozici neomezené množství dat za přijatelnou cenu nebo by je pro svou činnost nepotřeboval, či v případě mobilního připojení k internetu, které je zpravidla omezeno co do množství poskytovaných dat za určité časové období a zároveň je stále relativně nákladné.

2.2.2 Podmínky monitoringu

Podle stanoviska ÚOOÚ není zaměstnavatel oprávněn sledovat používání webových stránek zaměstnanci bez splnění podmínek § 316 odst. 2 ZP. Jako příklad závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele ÚOOÚ v kontextu sledování internetu uvádí např. mezinárodní bankovní převody či dozor nad prací vězňů; s takto restriktivním výkladem nesouhlasím – viz kapitolu 1.4 výše. ÚOOÚ dále tvrdí, že bez splnění podmínek § 316 odst. 2 ZP není zaměstnavatel oprávněn ani statisticky sledovat využívání přístupu k internetu ze strany zaměstnanců, např. doby

strávené surfováním po internetu.[144] Tento závěr podle mého názoru neobstojí v případě, kdy by taková obecná statistika nebyla nijak přiřaditelná ke konkrétním zaměstnancům, ale zaměstnavatel by ji sledoval pro všechny zaměstnance bez rozdílu společně. Domnívám se, že v takovém případě by nedocházelo k narušování soukromí jednotlivých zaměstnanců. Tuto praxi obecně zmiňuje též Pracovní skupina, přičemž zdůrazňuje, že se v této souvislosti nebude jednat o zpracování osobních údajů.[145] Přehled o využívání internetu a času stráveném návštěvou určitých stránek by pak zaměstnavatel mohl využít k rozhodnutí o blokaci některých stránek nebo o zákazu jejich navštěvování ze strany zaměstnanců během pracovní doby.

Poměrně neortodoxní názor zastává Jouza; tvrdí, že pokud zaměstnanci v pracovní době vyhledávají internetové stránky (jinak než za účelem výkonu práce), hrají hry a jinak zneužívají služební počítače, ochrana osobnosti se neuplatní a zaměstnavatel nepotřebuje ke kontrole takového jednání vydat opatření, v němž by vymezil závažný důvod spočívající v jeho zvláštní činnosti.[146] S tímto závěrem by dle mého názoru bylo možné souhlasit pouze v případě, kdy by se jednalo pouze o přiměřenou kontrolu dodržování zákazu užívání pracovních prostředků zaměstnavatele pro soukromé účely ve smyslu § 316 odst. 1 ZP. Pokud by však taková kontrola vykazovala prvky soustavnosti, pak by pro její výkon zaměstnavatel podmínky dle § 316 odst. 2 ZP splnit musel.

Pracovní skupina v kontextu sledování využití internetu ze strany zaměstnanců opakovaně zdůrazňuje, že zaměstnavatel by měl upřednostňovat prevenci zneužívání připojení k internetu před jeho odhalováním. Preventivní technická opatření jsou v případě kontroly užívání internetu dle názoru Pracovní skupiny schopna chránit zájmy zaměstnavatele lépe než nástroje k odhalování případů zneužívání, na něž musí zaměstnavatel vynakládat více energie a prostředků.[147] Pracovní skupina dokonce tvrdí,

---

144 ÚOOÚ: Stanovisko č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště, s. 4. Únor 2009.

145 Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 8/2001 o zpracování osobních údajů v kontextu zaměstnání (v originále: „*Opinion 8/2001 on the processing of personal data in the employment context*“) ze dne 13. září 2001, s. 13.

146 JOUZA, Ladislav. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. *Bulletin advokacie*. 2014, č. 6, s. 28. ISSN 1210-6348.

147 Např. viz Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Pracovní dokument o sledování elektronických komunikací na pracovišti (v originále: „*Working document on the surveillance of*

že v případech, kdy může zaměstnavatel zabránit zneužívání internetu např. užíváním webových filtrů (jež umožňují blokaci některých stránek), nemá obecně právo zaměstnance při užívání internetu sledovat, a to s ohledem na principy proporcionality a minimalizace rozsahu shromažďovaných osobních údajů.[148] Pokud užívání webových filtrů k ochraně zájmů zaměstnavatele nestačí, a ten proto přistoupí ke sledování užívání internetu, pak bude dle Pracovní skupiny ve většině případů k odhalení zneužívání internetu dostačující sledování názvu navštívených internetových stránek včetně času stráveného jejich prohlížením, tj. bez sledování obsahu těchto stránek. Teprve poté, co taková kontrola odhalí zneužívání připojení k internetu, je zaměstnavatel oprávněn zvažovat možnost dalšího sledování s ohledem na hrozící rizika. Pracovní skupina rovněž v kontextu sledování zneužívání internetu varuje před ukvapenými závěry, k nimž by zaměstnavatelé mohli relativně snadno dojít. Je třeba brát v úvahu, že některé stránky může zaměstnanec navštívit prakticky omylem – jednoduše přes různé vyhledávače, které jej na ně chybně odkážou (přičemž zaměstnanec hledal informaci, kterou potřebuje k plnění svých pracovních povinností), skrz nejasné či nesprávně uvedené hypertextové odkazy, v důsledku chybného zadání internetové adresy či nezamýšleného kliknutí na reklamní banner umístěný na stránce, kterou k plnění pracovních povinností potřebuje.[149]

Zaměstnavatel může v rámci preventivních opatření např. blokovat vymezené internetové stránky (typicky pornografické a jiné stránky s nevhodným obsahem, sociální sítě, seznamovací portály, chatovací místnosti, nákupní a herní portály, stránky umožňující zaměstnancům přístup do soukromé e-mailové schránky, internetové bankovnictví apod.), zakázat stahování jakýchkoli programů bez předchozí autorizace ze strany zaměstnance odpovědného za správu sítě, zablokovat možnost sledování videí (ať už na youtube.com či zpravodajských portálech včetně oblíbených přímých přenosů ze sportovních utkání), apod. Zejména v případě menších zaměstnavatelů však může být

---

electronic communications in the workplace") ze dne 29. května 2002, s. 24; a Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*") ze dne 8. června 2017, s. 15.

148 Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*") ze dne 8. června 2017, s. 23.

149 Vše v: Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Pracovní dokument o sledování elektronických komunikací na pracovišti (v originále: „*Working document on the surveillance of electronic communications in the workplace"*) ze dne 29. května 2002, s. 24.

zavedení takových preventivních opatření spojeno s vynaložením nemalých nákladů. Tehdy nelze dle Morávka na přijetí těchto opatření trvat a zaměstnavatel bude (po splnění informační povinnosti a dodržení dalších zásad monitoringu – viz kapitolu 1.5.2 výše) oprávněn monitorovat užití internetu ze strany jednotlivých zaměstnanců v rozsahu datum, čas a délka přístupů na internetové stránky a míra aktivity na nich, ovšem pouze ve vztahu k těm, které zaměstnanci primárně nepotřebují k plnění pracovních úkolů. I tato poslední podmínka nicméně odpadne, pokud by pro zaměstnavatele znamenala nepřiměřené náklady.[150] V dostupné literatuře jsem nenalezla výslovně formulovaný závěr, že by byl zaměstnavatel oprávněn sledovat též obsah internetových stránek navštívených zaměstnancem. S ohledem na výše citované stanovisko Pracovní skupiny se domnívám, že by tak teoreticky mohl činit v případě, kdy by neměl pro ochranu svých zájmů při splnění testu proporcionality jiného východiska. V každém případě však zaměstnavatel nebude oprávněn zpracovávat případné soukromé přihlašovací údaje a hesla zadávaná zaměstnancem na těchto internetových stránkách.

Informace o možnostech užívání internetu by měla být zaměstnancům pro vyloučení všech případných pochybností přístupná ve vnitřním předpise. Zaměstnavatel by zde měl popsat, zda vůbec zaměstnanci mohou využívat internet též pro soukromé účely, případně v jakém rozsahu (např. po ukončení pracovní doby, během přestávky v práci na jídlo a oddech nebo i během pracovní doby po určitý omezený počet hodin měsíčně apod.). Dále by vnitřní předpis měl v případě zavedení preventivních opatření specifikovat, jaké typy internetových stránek budou blokovány nebo k jakým stránkám budou mít zaměstnanci omezený přístup (tj. které stránky budou na tzv. blacklistu). Zaměstnavatel může jít i opačnou cestou, tj. naopak určit seznam stránek, které zaměstnanci mohou v pracovní době navštěvovat (tzv. whitelist); to však nebude v případě většiny zaměstnavatelů praktické, neboť zpravidla předem sotva odhadnou, jaké stránky budou jejich zaměstnanci potřebovat k plnění svých pracovních úkolů (v řadě situací mohou zaměstnanci získat cenné informace též na různých diskuzních

[150] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, dostupné elektronicky v systému ASPI. Část V., kapitola 2.1.2.1. ISBN 978-80-7478-139-1.

fórech, přitom charakter těchto stránek by většině zaměstnavatelů velel je preventivně zablokovat).

Jak doporučuje Pracovní skupina, zaměstnavatel by měl zaměstnance informovat o případném překročení oprávnění ohledně užívání internetu ideálně ihned v okamžiku, kdy k němu dojde, např. pomocí automatického přesměrování na stránku s upozorněním na detekci zneužití přístupu k internetu. Taková praxe by dle Pracovní skupiny pomohla vyřešit mnohá nedorozumění, k nimž v oblasti užívání internetu ze strany zaměstnanců nutně dochází.[151] Toto opatření je vhodné i dle mého názoru, nicméně většina velkých zaměstnanců zřejmě raději zvolí cestu blokace určitých internetových stránek, zatímco pro menší zaměstnavatele může i takové řešení představovat neúměrnou zátěž.

2.2.3 Konkrétní příklady scénářů monitoringu činnosti zaměstnanců na internetu

(a) Blokace nepracovních internetových stránek

V tomto scénáři mějme zaměstnavatele, který zaměstnancům vůbec nepovolí užívání internetu pro soukromé potřeby a zvolí cestu blokace vybraných nepracovních stránek. Zaměstnavatel může určit tzv. whitelist, tj. vymezený seznam internetových stránek, které zaměstnanci potřebují k výkonu své práce, přičemž všechny ostatní stránky zablokuje. Pracovní skupina sice tvrdí, že úplný zákaz užívání internetu pro soukromé účely zaměstnanců lze považovat za nepraktický a poměrně nereálný, neboť nebere v úvahu způsob, jakým může internet zaměstnancům pomáhat v každodenním pracovním životě[152], přesto však jistě existuje řada pracovních pozic, na nichž zaměstnanci ke své práci reálně potřebují jen omezený a předem známý výčet internetových stránek. Může se jednat o zaměstnance zpracovávající určité veřejně dostupné informace z obchodního či insolvenčního rejstříku, zaměstnance poskytující online podporu zákazníkům ohledně produktů zaměstnavatele nabízených na internetu, zaměstnance spravující internetové stránky zaměstnavatele, apod. Pokud se

[151] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Pracovní dokument o sledování elektronických komunikací na pracovišti (v originále: „*Working document on the surveillance of electronic communications in the workplace"*) ze dne 29. května 2002, s. 15.

[152] Tamtéž, s. 24.

zaměstnanec bude domnívat, že ke své práci potřebuje přístup na jiné než whitelistem povolené stránky, měl by za tímto účelem kontaktovat svého nadřízeného zaměstnance, který situaci posoudí a případně nechá danou stránku zpřístupnit.

Druhou cestou, kterou může zaměstnavatel v tomto scénáři zvolit, je tzv. blacklist, tj. blokace vybraných internetových stránek, jejichž typologie bude uvedena ve vnitřním předpise a o nichž lze s přehledem říci, že je zaměstnanci ke své práci skutečně nepotřebují. Jakmile se zaměstnanec pokusí na takto zablokovanou internetovou stránku připojit, bude přesměrován na stránku s informací, že se jedná o stránku blokovanou v souladu s vnitřním předpisem.

V obou případech půjde zaměstnavatel výlučně cestou zavedení preventivních opatření, jak požaduje Pracovní skupina. Dodatečné sledování navštívených internetových stránek by v tomto scénáři nebylo pro ochranu zájmů zaměstnavatele nutné, tudíž by je zaměstnavatel neměl provádět.[153]

(b) Omezené užívání internetu pro soukromé účely a následná blokace

V tomto scénáři mějme relativně benevolentního zaměstnavatele, který zaměstnancům povolí užívání internetu pro soukromé účely v rozsahu nejvýše 12 hodin za kalendářní měsíc. Časomíra bude nastavena automaticky a poběží v případě, kdy zaměstnanec z pracovního počítače navštíví určité internetové stránky, jejichž okruh bude předem vymezen ve vnitřním předpise a které k výkonu práce zjevně nejsou potřeba (např. youtube.com, sociální sítě, soukromý e-mail, nákupní portály). Čas se bude odečítat bez ohledu na skutečnost, zda zaměstnanec internet pro soukromou potřebu využije během pracovní doby, po ní nebo během přestávky na jídlo a oddech. Jakmile zaměstnanec v daném měsíci vyčerpá povolený rozsah takového užívání internetu, bude na tuto skutečnost upozorněn prostřednictvím přesměrování na informační stránku. Následně budou tyto vymezené internetové stránky po zbytek příslušného kalendářního měsíce zablokovány.

---

[153] Viz Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 23, a rovněž MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, dostupné elektronicky v systému ASPI. Část V., kapitola 2.1.2.1. ISBN 978-80-7478-139-1.

Tento scénář může být technicky náročnější. Při běhu časomíry by zaměstnavatel neměl sledovat, jaké konkrétní stránky zaměstnanec navštěvuje a jak dlouho; jakýkoli sběr dat by se měl omezit pouze na celkový čas strávený prohlížením určitého agregovaného množství stránek. Po uplynutí dovoleného času by se také nabízela možnost zahájit monitoring dodržování zákazu navštěvování vymezených internetových stránek. Řešení pomocí jejich blokace však považuji za vhodnější; jestliže má zaměstnavatel technické podmínky pro nastavení časomíry na využití určitých stránek, jistě bude schopen zajistit jejich následnou blokaci jako preventivní opatření, které má mít před monitoringem přednost.

(c) Zákaz užívání internetu pro soukromé účely se soustavnou kontrolou jeho dodržování

V tomto scénáři mějme zaměstnavatele zaměstnávajícího pouze několik zaměstnanců, který jim užívání internetu pro soukromé účely nepovolí. Ve vnitřním předpise je výslovně upozorní, že navštěvování stránek s nevhodným obsahem, herních a stahovacích portálů, sociálních sítí a soukromých elektronických schránek bude s ohledem na síťovou bezpečnost soustavně monitorováno v rozsahu datum, čas a délka strávená jejich prohlížením. S ohledem na zajištění řádného provozu systému bude ve stejném rozsahu rovněž soustavně monitorováno sledování videí na youtube.com a podobných internetových stránkách, včetně zpravodajských serverů. Zaměstnanci budou zároveň upozorněni, že užívání internetového připojení pro soukromé účely bude moci být považováno za porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci s důsledky odpovídajícími závažnosti takového porušení.

V tomto scénáři se zaměstnavatel rozhodl pro zavedení monitoringu, neboť s ohledem na malý počet zaměstnanců by pro něho bylo řešení pomocí blokace vybraných internetových stránek nepoměrně nákladné.

2.2.4 Relevantní rozhodovací praxe

(a) Evropský soud pro lidská práva

Sledování užívání internetu ze strany zaměstnance se Evropský soud pro lidská práva věnoval v již výše popisovaném případě Coplandová proti Spojenému království (rozsudek ze dne 3. dubna 2007). Obecné okolnosti případu a závěry soudu ohledně porušení práva paní Coplandové na soukromí uvádím v kapitole 2.1.4(a) výše. Co se týče sledování internetu jako takového, pak dodejme, že bylo ze strany zaměstnavatele prováděno v rozsahu název navštívené stránky, datum, čas a doba trvání jejího prohlížení. Celý monitoring dle vyjádření zaměstnavatele trval po dobu jednoho měsíce, zatímco zaměstnankyně tvrdila, že musel trvat mnohem déle. Pro účely rozhodnutí soudu však nebyla délka trvání monitoringu dále prokazována.[154]

V kontextu užívání internetu během pracovní doby je rovněž zajímavé částečně disentní stanovisko soudce Paula Pinta de Albuquerque k případu Bărbulescu proti Rumunsku (rozsudek ze dne 12. ledna 2016, podrobnější popis viz kapitola 1.4 výše). V něm soudce formuloval závěr, že v současné době zosobňuje internet prostor pro uplatnění práva na svobodu projevu, jaký nemá obdoby, a rovněž hraje důležitou roli v oblasti posilování přístupu veřejnosti k informacím a k jejich šíření. V tomto smyslu by proto měl být přístup k internetu chápán jako součást výše jmenovaných základních práv a svobod. Státy by měly usilovat o rozvíjení možností přístupu k internetu a o budování odpovídající infrastruktury a zároveň garantovat s tím související ochranu soukromí uživatelů internetu. Soudce dochází k poměrně neortodoxnímu závěru, že je nepřípustné, aby zaměstnavatel zaměstnancům zcela zakázal užívání internetu pro soukromé účely, stejně jako aby zavedl plošné, automatické a soustavné sledování užívání internetu ze strany zaměstnanců. Zaměstnanci mají být informováni o pravidlech užívání internetu a dle názoru soudce s těmito pravidly musejí výslovně souhlasit. Zaměstnavatel by měl být oprávněn shromažďovat osobní údaje v souvislosti s užíváním internetu pouze výjimečně a s přivolením soudu (pokud s takovým shromažďováním údajů nedá souhlas sám zaměstnanec), neboť se zaměstnanci podezřelými z porušování vnitřních předpisů zaměstnavatele nemá být zacházeno hůře

[154] Rozsudek Evropského soudu pro lidská práva, stížnost č. 62617/00, ze dne 3. dubna 2007, Věc Coplandová proti Spojenému království.

než s obviněnými osobami v trestním řízení (jak tomu dle názoru soudce zřejmě v tomto ohledu je). Soudce zdůrazňuje, že sledovací opatření mají být zavedena pouze v případě řádně odůvodněného podezření zaměstnance z porušování vnitřních předpisů.[155]

Výše uvedené názory sice přinášejí zcela nový pohled na problematiku užívání internetu, na druhou stranu jsou v současné době zřejmě předčasné. Nedomnívám se, že by omezení užívání internetu na pracovišti představovalo zásadní omezení práva zaměstnanců na svobodu projevu a přístupu k informacím; zaměstnanci zcela jistě mohou potřebu těchto práv saturovat mimo svou pracovní dobu a ze svých vlastních prostředků. Naopak takový výklad pomíjí právo zaměstnavatele jako vlastníka pracovních prostředků možnost určovat, jakým způsobem s nimi má být zacházeno.[156] Nelze ovšem zřejmě vyloučit, že v budoucnu povede výklad směrem, který naznačil právě soudce Pinto de Albuquerque.

(b) ÚOOÚ a soudy České republiky

Z české rozhodovací praxe uveďme usnesení Ústavního soudu sp. zn. I. ÚS 452/09 ze dne 31. března 2009, kde soud kromě jiného formuloval hojně citovaný závěr ohledně limitů práva na soukromí na pracovišti, jenž zmiňuji výše (viz kapitolu 1.1 poslední odstavec). V posuzovaném případě stěžovatelka namítala, že zaměstnavatel porušil její právo na listovní tajemství pořízením detailního výpisu o připojení jejího služebního počítače na internet. Ten byl následně proti ní použit v trestním řízení, v němž byla uznána vinnou trestným činem poškozování cizích práv. Výpis obsahoval seznam navštívených stránek včetně uvedení času jejich prohlížení. Ústavní soud konstatoval, že v tomto případě k zásahu do práva stěžovatelky na listovní tajemství dle čl. 13 Listiny základních práv a svobod nedošlo, neboť „*stěžovatelka provedla připojení na zmíněné webové stránky ze služebního počítače, určeného k plnění pracovních povinností, umístěného v budově a kanceláři svého zaměstnavatele, který v rámci bezpečnostního systému monitoruje připojení na internet, což bylo stěžovatelce jistě*

---

[155] Rozsudek Evropského soudu pro lidská práva, stížnost č. 61496/08, ze dne 12. ledna 2016, Věc Bărbulescu proti Rumunsku, částečně disentní stanovisko soudce Pinta de Albuquerque.

[156] Shodně též NONNEMANN, František. Sledování aktivity zaměstnance na internetu ve světle aktuální judikatury Evropského soudu pro lidská práva [online]. Publikováno dne 2. února 2016 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.epravo.cz/top/clanky/sledovani-aktivity-zamestnance-na-internetu-ve-svetle-aktualni-judikatury-evropskeho-soudu-pro-lidska-prava-100316.html>.

známo a byla srozuměna s tím, že výpis z bezpečnostního sytému obsahuje report webové stránky, včetně konkrétního uživatelského jména (doménového účtu), které se na danou webovou stránku připojilo.“[157] Případ byl však posuzován ještě za účinnosti předchozího zákoníku práce (zákon č. 65/1965 Sb.), který úpravu obdobnou dnešnímu § 316 ZP neobsahoval.

Dále se kontrolou užívání internetu ze strany zaměstnanců zabýval Nejvyšší soud; v obou případech se však jednalo o kontrolu zákazu užívání výrobních a pracovních prostředků zaměstnavatele pro soukromou potřebu dle § 316 odst. 1 ZP, a nikoli o soustavný monitoring dle § 316 odst. 2 ZP.

Velmi diskutovaným je rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1771/2011 ze dne 16. srpna 2012; případ se následně dostal k Ústavnímu soudu, který o něm rozhodl usnesením sp. zn. I. ÚS 3933/12 ze dne 7. listopadu 2012. Okolnosti případu a obě tato rozhodnutí popisuji již v kapitole 1.5.2(b) výše. Zde jen pro přehlednost zopakuji svůj názor, že (skryté) sledování zaměstnance trvající nepřetržitě po celý jeden měsíc vykazuje prvky soustavného sledování, a proto měly být splněny podmínky § 316 odst. 2 a 3 ZP. Nejvyšší soud však v tomto rozhodnutí konstatoval, že ustanovení § 316 odst. 2 ZP se vztahuje „*jen na situace, kdy zaměstnanec buď se souhlasem zaměstnavatele používá pro svou osobní potřebu zaměstnavatelovy výrobní a pracovní prostředky, nebo z nějakého důvodu používá u zaměstnavatele své vlastní výrobní a pracovní prostředky včetně výpočetní techniky či telekomunikačního zařízení, a na všechny předměty a projevy soukromé povahy zaměstnance. V projednávané věci se přitom jednalo o kontrolu dodržování zákazu uvedeného v § 316 odst. 1 ZP, jejíž výkon zákon zaměstnavateli umožňuje, a nikoli o sledování soukromých aktivit zaměstnance; míra zásahu do soukromí žalobce byla zcela zanedbatelná*.“ Musím říci, že výkladu, proč by se § 316 odst. 2 ZP měl vztahovat pouze na výše uvedené situace, nerozumím. Takový závěr dle mého názoru z daného ustanovení nevyplývá a Nejvyšší soud ve svém rozhodnutí ani blíže neuvedl, jak k němu došel.[158]

Další případ kontroly užívání internetu ve smyslu § 316 odst. 1 ZP řešil Nejvyšší soud v rozsudku sp. zn. 21 Cdo 747/2013 ze dne 7. srpna 2014. Zaměstnavatel se

[157] Usnesení Ústavního soudu sp. zn. I. ÚS 452/09 ze dne 31. března 2009.

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

zaměstnancem rozvázal pracovní poměr podle § 52 písm. f) a g) ZP, neboť v pracovní době v celkem třech po sobě jdoucích dnech vyhledával na internetu prostřednictvím firemního počítače informace pro soukromé účely; dále v pracovní době ve dnech 20. ledna až 19. února 2010 zneužil přidělený firemní telefon pro soukromé účely (a pro úplnost, jednou se bez omluvy dostavil na pracoviště o 20 minut později). Na možnost výpovědi byl zaměstnanec dvakrát písemně upozorněn.

Co se týče užívání internetu, bránil se zaměstnanec tím, že jej takto použil právě pouze ve třech dnech a navíc za situace, kdy mu nebyla přidělována práce v souladu s pracovní smlouvou. Dále zaměstnanec uvedl, že zaměstnavatel provedením kontroly způsobu použití pracovních prostředků porušil ustanovení § 316 odst. 2 ZP. Tento názor Nejvyšší soud nepodpořil s tím, že „*cílem (smyslem) kontroly prováděné zaměstnavatelem (žalovaným) nebylo zjišťování obsahu telefonátů žalobce, nýbrž toliko zjištění, zda zaměstnanec (žalobce) respektuje (a když nerespektuje, tak v jaké míře) zákaz užívat pro svou osobní potřebu přidělený počítač zaměstnavatele (žalovaného), popřípadě přidělený služební telefon*.“ Výpověď tak shledal platnou.[159]

Ačkoli se v rozhodnutí neuvádí, jakým způsobem byla kontrola užívání internetu provedena, tak za předpokladu, že zaměstnavatel provedl namátkovou kontrolu ve třech po sobě jdoucích dnech, se závěry Nejvyššího soudu souhlasím. Takto časově omezená kontrola bude dle mého názoru pro účely § 316 odst. 1 ZP přiměřená a zaměstnavatel pro její provedení nemusí splnit podmínky § 316 odst. 2 a 3 ZP.

2.3 Kamerový systém

2.3.1 Úvodní poznámky

Kamerové systémy jsou považovány za velmi invazivní prostředek monitoringu. Umožňují totiž v reálném čase pozorovat jednání zaměstnance, čímž také do jisté míry toto jednání ovlivňují. Jak zdůraznil Nejvyšší správní soud, „*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*

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

schopny naplnit vytyčený účel, který je sledován. Je zcela nepochybné, že kamerový systém ve srovnání s jinými prostředky (např. personálními, mechanickými), které mohou dosáhnout naplnění účelů žadatelem sledovaných, zasahuje základní lidská práva, a to právo na soukromí a na soukromý rodinný život, která jsou garantována čl. 10 Listiny základních práv a svobod a v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod, a tudíž i do lidské důstojnosti, z které tato práva vyplývají… Městský soud shodně s žalovaným (pozn.: ÚOOÚ) *upřednostnili zájem na ochranu soukromí (jako jedno ze základních lidských práv) před zájmem na ochraně majetku s tím, že postup stěžovatele, který nadřadil zájem na ochraně před drobnými krádežemi, vandalstvím a případným excesem některého z návštěvníků nad právo na ochranu soukromí a osobního života, je nepřípustný a především neproporcionální.*“[160] Zdálo by se tedy, že v případě kamerových systémů by mělo být obtížnější splnit test proporcionality.

Jako závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele ve smyslu § 316 odst. 2 ZP může za dodržení principu proporcionality obstát např. ochrana majetku zaměstnavatele, ochrana zdraví a bezpečnosti zaměstnanců a dle mého názoru též kontrola dodržování technologických postupů (např. při výrobě léčiv, v jaderné elektrárně a v dalších obdobně nebezpečných provozech). Nepřípustné by však dle Pracovní skupiny bylo zavedení kamerových systémů přímo a pouze za účelem kontroly kvality a objemu vykonané práce, se snímáním ze vzdáleného místa; jinak by tomu však bylo, pokud by účelem kontroly bylo dodržování bezpečnostních opatření ke splnění požadavků na výrobu nebo bezpečnost při práci.[161] Obdobně i Evropský inspektor ochrany údajů, nezávislá instituce pro ochranu osobních údajů v Evropské unii, upozorňuje, že zavedení kamerových systémů pro účely sledování výkonu práce by obecně nemělo být přípustné, s výjimkou případů, kdy zaměstnavatel prokáže, že jeho zájem na takovém sledování převáží nad zájmy zaměstnanců. Dále uvádí následující ilustrační případy, kdy by monitoring neměl být prováděn: (i) pro účely sledování výkonu práce uklízečky, přestože o něm byla informována a před zahájením monitoringu byly zaznamenány stížnosti ohledně její práce, a (ii) pro účely soustavného

[160] Rozsudek Nejvyššího správního soudu sp. zn. 5 As 158/2012 ze dne 23. srpna 2013.

[161] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 25.

sledování pokladní a pokladny v jídelně během otevírací doby, opět přes předchozí informaci o takovém monitoringu.[162]

I přesto, že by zaměstnavatel argumentoval ochranou majetku, nebyl by však oprávněn kamerové systémy instalovat např. do šaten zaměstnanců bez vymezení nesledovaného prostoru pro převlékání s odůvodněním, že zaměstnanci se dopouštějí krádeží a právě při převlékání tyto odcizené věci viditelně ukrývají do tašek, což lze odhalit právě pomocí kamerového systému.[163] Totéž samozřejmě platí o dalších prostorech určených k ryze soukromým úkonům, jako jsou např. toalety, sprchy a místa vyhrazená k odpočinku zaměstnanců.[164]

Jak konstatuje Pracovní skupina, současné technologie v oblasti snímání obrazu přinášejí pro soukromí zaměstnanců dříve neznámé hrozby. Záznamy z kamerových systémů mohou být totiž velice jednoduše přístupné dálkově např. pomocí chytrých telefonů, kamery mohou být co do velikosti zanedbatelné a přesto schopné pořizovat záznamy ve vysokém rozlišení a technické prostředky umožňují dříve neznámé možnosti, např. automatické rozpoznávání obličeje. Tato funkce by sice mohla zaměstnavatelům pomoci např. sledovat, zda se konkrétní zaměstnanci neoprávněně nepohybují v jiné než vymezené části pracoviště, avšak s ohledem na princip proporcionality, možnost profilování a automatizovaného rozhodování by se měli zaměstnavatelé jejímu užívání zásadně vyhnout.[165] Dle čl. 4 odst. 14 GDPR navíc zobrazení obličeje představuje biometrický údaj, jehož zpracování za účelem jedinečné identifikace fyzické osoby je dle čl. 9 odst. 2 GDPR možné pouze za vymezených podmínek, mezi něž ochrana práv a právem chráněných zájmů zaměstnavatele nespadá (k tématu monitoringu pomocí zpracování biometrických údajů viz též kapitolu 2.6.1 níže).

---

[162] EDPS: Zásady video monitoringu vydané EDPS (v originále: „*The EDPS Video-Surveillance Guidelines*“). Brusel, 17. března 2010, s. 22.

[163] BARTÍK, V., JANEČKOVÁ, E. *Kamerové systémy v praxi*. 1. vyd. Praha: LINDE, 2011, dostupné elektronicky v systému ASPI. Kapitola 1.2. ISBN 978-80-7201-850-5.

[164] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 25.

[165] Tamtéž, s. 19.

Při monitoringu pomocí kamerových systémů je dále třeba vzít v úvahu úpravu obsaženou v OZ. Dle § 84 OZ lze zachytit podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, jen s jeho svolením; svolení nicméně dle § 88 odst. 1 OZ není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použije k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob. Dodejme ještě, že dle § 90 OZ nesmí být tento zákonný důvod využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka; i OZ tudíž zdůrazňuje princip proporcionality.

2.3.2 Podmínky monitoringu a jeho základní způsoby

Monitoring pomocí kamerového systému může být provozován ve dvou režimech: se záznamem pořizovaných záběrů a bez takového záznamu; oba tyto scénáře jsou podrobněji popsány v podkapitolách níže. Pro rozhodnutí, který z těchto systémů může být s ohledem na princip proporcionality zaveden, je třeba zvážit konkrétní okolnosti dané u zaměstnavatele a účel instalace kamerového systému. Jak konstatuje Pracovní skupina, v některých případech bude dostačující systém umožňující zobrazení záběrů na uzavřeném okruhu bez jejich zaznamenávání (např. u pultů v supermarketech), v jiných bude možné odůvodnit pořizování záznamů a jejich uchovávání; také doba uchování musí být podrobena testu proporcionality.[166]

Pracovní skupina rovněž zdůrazňuje, že s ohledem na principy přiměřenosti a omezení rozsahu zpracovávaných osobních údajů by měly být při instalaci kamerového systému vzaty v úvahu zejména následující parametry: (i) nastavení úhlů záběrů všech kamer s ohledem na vymezený účel užívání kamerového systému (kamery by neměly snímat detaily, jež nejsou pro daný účel nezbytně nutné), (ii) druh snímacího zařízení, tj. zda se bude jednat o stacionární či pohyblivé kamery, (iii) vlastní umístění kamer, nastavení jejich pohybu apod. (jak konstatoval Nejvyšší správní soud, monitoring pro účely ochrany majetku zaměstnavatele musí být směřován na tento majetek, nikoli na osobu

[166] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 4/2004 o zpracování osobních údajů pomocí kamerových systémů (v originále: „*Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*“) ze dne 11. února 2004, s. 20.

zaměstnance[167]), (iv) možnosti zvětšování a/nebo přibližování snímaného obrazu, a to již během samotného snímání nebo později při sledování pořízených záznamů, a dále možnosti rozmazání či vymazání jednotlivých obrazů, (v) funkce zmrazení snímaného obrazu, (vi) spojení s centrálou za účelem vysílání zvukových či obrazových varování, a (vii) kroky, jež mají být učiněny v důsledku kamerového sledování, např. uzavření vstupu, přivolání odpovědného zaměstnance, apod.[168] Podrobnější doporučení pak uvádí Evropský inspektor ochrany údajů a patří mezi ně např. omezení počtu kamer na nezbytné minimum, omezení záběrů kamer a času jejich provozního režimu s ohledem na stanovený účel jejich instalace a používání kamer jen s nezbytně potřebným rozlišením obrazu.[169]

Kromě vnitropodnikové směrnice, která bude podrobně popisovat monitoring pomocí kamerového systému, by měl zaměstnavatel též označit monitorované prostory informačními tabulkami. Ty by měly být umístěny tak, aby byli zaměstnanci a případné třetí osoby (např. zákazníci) na kamerový systém upozorněni ještě před vstupem do monitorovaných prostor, tj. před záběr příslušné kamery umístěné uvnitř prostoru. Informační tabulky by měly obsahovat alespoň piktogram kamery, údaj o tom, že je prostor monitorován, identifikaci správce a odkaz na místo nebo osobu, kde je možné získat o kamerovém systému více informací.[170]

(a) Kamerové systémy bez záznamu

Kamerový systém bez pořizování záznamu (ať již obrazového či zvukového) je logicky méně invazivním prostředkem monitoringu než kamerový systém se záznamem. Zároveň nepředstavuje zpracování osobních údajů, tudíž se neuplatní ZOOÚ a posléze GDPR. To ovšem znamená, že zaměstnavatel není povinen plnit podmínky, které stanoví ZOOÚ, respektive GDPR, např. náležité zabezpečení kamerového systému, omezení rozsahu sledování, atd. Tuto povinnost totiž nelze vyvodit, neboť analogická

[167] Rozsudek Nejvyššího správního soudu sp. zn. 5 As 158/2012 ze dne 23. srpna 2013.

[168] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 4/2004 o zpracování osobních údajů pomocí kamerových systémů (v originále: „*Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*“) ze dne 11. února 2004, s. 19 – 20.

[169] EDPS: Zásady video monitoringu vydané EDPS (v originále: „*The EDPS Video-Surveillance Guidelines*“). Brusel, 17. března 2010, s. 24 – 26.

[170] ÚOOÚ: Provozování kamerových systémů. Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů. Brno: Masarykova univerzita, 2012, s. 21. ISBN 978-80-210-6017-3.

aplikace předpisů na ochranu osobních údajů není možná s ohledem na skutečnost, že se jedná o veřejnoprávní předpisy a dle čl. 2 odst. 4 Ústavy České republiky nesmí být nikdo nucen činit, co zákon neukládá. Pochopitelně však lze zaměstnavateli přiměřenou aplikaci zásad ochrany osobních údajů jedině doporučit.[171] Bývalý veřejný ochránce práv, JUDr. Pavel Varvařovský (ve funkci v letech 2010 – 2013), v době výkonu své funkce konstatoval, že fakticky nejednotná regulace kamerových systémů není důvodná. Moderní informační technologie totiž umožňují, aby provozovatel kamerového systému přecházel z jednoho z těchto režimů provozu kamer do druhého, a to v podstatě jedním stisknutím tlačítka. Tato skutečnost přitom může mít významný dopad na vymahatelnost práva, neboť ÚOOÚ není v případě kamerových systémů bez záznamu oprávněn provádět kontrolu dodržování právních předpisů a zaměstnanec se musí svých práv domáhat v občanskoprávním řízení.[172] Je pravdou, že v řadě zemí Evropské unie existuje samostatná právní úprava kamerových systémů. Jisté pokusy o její zavedení byly učiněny také v České republice. V roce 2010 uplatnil ÚOOÚ v rámci aktivit Sekretariátu Rady vlády pro lidská práva vlastní návrh právní úpravy sledovacích (kamerových) systémů formou novelizace ZOOÚ.[173] Tento návrh nicméně nakonec přijat nebyl.

Dodejme však, že kamerové systémy bez pořizování záznamu nejsou v praxi příliš hojně užívány. Pokud má kamerový systém sloužit k ochraně majetku, je právě záznam z něj pořízený zpravidla užíván jako důkazní prostředek.

(b) Kamerové systémy se záznamem

Při použití tohoto typu kamerového systému je zpravidla pořizován pouze obrazový záznam snímaných záběrů. Pokud by zaměstnavatel zamýšlel současně pořizovat též zvukový záznam, musel by řádně zdůvodnit, že je taková praxe skutečně nezbytná pro ochranu jeho zájmů. Dle názoru ÚOOÚ představuje pořizování zvukového záznamu současně se záznamem obrazovým hrubý zásah do soukromí sledovaných osob. Ve většině případů totiž pro prokázání určitého sledu událostí zcela postačí pouze obrazový

---

171 Shodně též NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 235. ISSN 1210-6410.

172 ÚOOÚ: Informační bulletin 2/2011. Prosinec 2011, s. 16 – 17.

173 Tamtéž, s. 4.

záznam.[174] Specifickou úpravu v tomto směru nicméně obsahuje § 72 zákona o hazardních hrách, který provozovatelům heren a kasin ukládá povinnost své prostory vybavit zařízením umožňujícím po celou provozní dobu v reálném čase monitorovat vstup do herny nebo kasina a veškeré herní prostory. Monitorovací zařízení musí být vybaveno časovou a datovou funkcí a pořízený záznam musí být barevný, jasný, zřetelný a rozlišitelný; zároveň musí být pořizován též zvukový záznam, který nesmí být oproti monitorované skutečnosti zkreslený. Takto pořízené záznamy je provozovatel povinen uchovávat po dobu dvou let. Tato právní úprava dle mého názoru představuje skutečně významný zásah do soukromí fyzických osob, a to nejen návštěvníků těchto zařízení, ale především zaměstnanců, kteří v nich pracují.

Provádění záznamu pořizovaných záběrů představuje zpracování osobních údajů, pokud mají být využity k identifikaci fyzických osob v souvislosti s určitým jednáním. Totéž by platilo v případě, kdy by za stejným účelem byly v záznamovém zařízení uchovávány jiné informace než obrazový záznam. Dle stanoviska ÚOOÚ představují údaje uchovávané v záznamovém zařízení (ať už obrazové či zvukové) osobní údaje tehdy, pokud lze na jejich základě přímo či nepřímo identifikovat konkrétní fyzickou osobu, tj. ze snímku jsou patrné její charakteristické rozpoznávací znaky (zpravidla obličej), přičemž na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace této osoby.[175] Nebude-li proto záznam z kamerového systému možno doplnit dalšími informacemi, nelze dle ÚOOÚ údaje získané v obecné rovině vztáhnout k určitému nebo určitelnému subjektu údajů.[176] To však zřejmě nebude případ monitoringu zaměstnanců, neboť ty zaměstnavatel zná a z pořízených záběrů je schopen je zpravidla bez dalšího identifikovat. ÚOOÚ nicméně vyslovuje určitou presumpci dalšího využívání pořízených záběrů, i když nedosahují výše uvedené kvality osobních údajů; pokud by totiž neměly být tyto nijak využívány, jejich pořizování by logicky postrádalo jakýkoli smysl.[177] Lze totiž jen těžko vyloučit, že by k identifikaci

[174] ÚOOÚ: Provozování kamerových systémů. Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů. Brno: Masarykova univerzita, 2012, s. 8. ISBN 978-80-210-6017-3.

[175] ÚOOÚ: Stanovisko č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Leden 2006.

[176] ÚOOÚ: Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Leden 2006.

[177] Tamtéž.

osob na pořízených záznamech nemohlo dojít kdykoli v budoucnu, a proto se celý záznamový systém musí považovat za zpracovávání údajů o identifikovatelných osobách, i když některé osoby zachycené na záznamu identifikovatelné nejsou.[178]

V praxi také panovala určitá nejistota, zda pořizováním záznamů pomocí kamerového systému dochází zároveň ke zpracování citlivých údajů. Ze záběrů podoby fyzické osoby lze totiž často poznat její rasový nebo etnický původ, který představuje citlivý údaj dle § 4 písm. b) ZOOÚ, respektive patří do zvláštní kategorie osobních údajů dle čl. 9 odst. 1 GDPR. K této otázce zaujal ÚOOÚ stanovisko, že pokud nedochází k systematickému zpracovávání těchto údajů (tj. kamerový systém má odhalovat pachatele krádeží bez ohledu na jejich etnický původ), nepůjde o zpracování citlivých údajů.[179] Obdobně i recitál 51 GDPR říká, že by zpracování fotografií nemělo být systematicky považováno za zpracování zvláštních kategorií osobních údajů, neboť na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky. Tento závěr lze jistě vztáhnout též na obrazové záznamy pořízené kamerovým systémem.

Další otázkou je, jak dlouho mají být pořízené záznamy uchovávány. Dle Pracovní skupiny má samozřejmě záležet na individuálních podmínkách u daného správce údajů. V případě ochrany majetku zaměstnavatele tak bude ospravedlnitelné záznamy uchovávat po dobu několika hodin a následně je vymazat, např. automaticky na konci každého dne. Pokud však mají tyto záběry sloužit jako důkazní prostředek, mohou být pochopitelně uchovány po dobu nezbytnou k přijetí opatření ze strany policejních či soudních orgánů. Má-li ovšem správce údajů v úmyslu uchovávat záznamy po delší dobu než po několik hodin, může tak činit pouze po pečlivé aplikaci principu proporcionality, přičemž tato doba by neměla být delší než jeden týden.[180] Obdobný

---

[178] BARTÍK, Václav, JANEČKOVÁ, Eva. Kamery se záznamovým zařízením na pracovišti. *Práce a mzda*. 2010, č. 3. ISSN 0032-6208. Dostupné z WWW: <http://www.mzdovapraxe.cz/archiv/dokument/doc-d9135v11954-kamery-se-zaznamovym-zarizenim-na-pracovisti/?search_query=%24issue%3D3I97&order_by=&order_dir=&type=&search_results_page=1>.

[179] ÚOOÚ: Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Leden 2006.

[180] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 4/2004 o zpracování osobních údajů pomocí kamerových systémů (v originále: „*Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*“) ze dne 11. února 2004, s. 20.

názor sdílí ÚOOÚ; doba uchování údajů by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému a v zásadě by neměla přesahovat několik dnů. V případě trvale střežených objektů se nabízí uchovávání dat v rámci časové smyčky v délce např. 24 hodin s tím, že poté mají být záznamy automaticky smazány.[181] V již výše vzpomínaném návrhu specifické právní úpravy kamerových systémů měl ÚOOÚ v úmyslu zakotvit pravidlo, že pokud by záznamy byly uchovávány déle než tři pracovní dny od jejich pořízení, bylo by zpravidla nutné vyhotovit písemné zdůvodnění, proč a po jakou dobu má být záznam uchováván pro účely ochrany majetku a osob před protiprávním jednáním nebo pro účely postihu takového jednání, a toto zdůvodnění uchovávat nejméně po dobu uchovávání pořízeného záznamu.[182]

Pracovní skupina zdůrazňuje, že záznamy pořízené za účelem ochrany majetku zaměstnavatele a/nebo prevence a odhalování závažných provinění by neměly být použity k trestání zaměstnanců za nezávažná porušení pracovní kázně. Zároveň by dotčeným zaměstnancům mělo být umožněno použít pořízené záběry pro účely uplatňování vlastních námitek a tvrzení v případě, že mají být použity proti nim.[183]

2.3.3 Konkrétní příklady scénářů monitoringu pomocí kamerového systému

(a) Kamerový systém bez záznamu s online přenosem

Zaměstnavatel v tomto scénáři je výrobcem automobilových dílů, při jejichž výrobě se nakládá s mědí a dalšími kovy. V minulosti docházelo k řadě případů krádeží těchto kovů i přesto, že při opouštění areálu zaměstnavatele byli zaměstnanci podrobováni prohlídce pomocí detektoru kovů. Proto se zaměstnavatel rozhodl pro instalaci

[181] ÚOOÚ: Stanovisko č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Leden 2006.

[182] Zdůvodnění by nebylo třeba vyhotovit pokud: a) záznam dokumentuje buď způsobení škody na majetku anebo újmu na zdraví či životě osoby, anebo b) záznam dokumentuje jiné jednání, které bylo předmětem buď trestního oznámení anebo návrhu či podnětu k zahájení správního řízení anebo návrhu na zahájení občanskoprávního řízení, anebo c) záznam nezachycuje fyzické osoby. Viz ÚOOÚ: Informační bulletin 2/2011. Prosinec 2011, s. 5.

[183] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 25.

kamerového systému. Kamery jsou zaměřeny na zdi kolem areálu továrny, kde zaměstnanci přicházejí do styku s kovy, jsou v provozu po celou pracovní dobu a jejich online přenos nepřetržitě sleduje hlídač. S existencí kamerového systému jsou zaměstnanci předem seznámeni prostřednictvím vnitřního předpisu a v prostorách před vstupem do monitorovaného prostoru jsou rovněž umístěny informační tabulky upozorňující na monitoring. V případě, že kamera zaznamená zaměstnance, který se snaží opustit areál mimo vyznačené východy (zřejmě s cílem vyhnout se detektoru kovů), je na místo vyslán hlídač s detektorem kovů a zaměstnance podrobí prohlídce.

(b) Kamerový systém se záznamem uchovávaným po dobu několika hodin

V tomto scénáři mějme zaměstnavatele, který za účelem kontroly dodržování bezpečnosti a ochrany zdraví při práci instaluje kamerový systém do laboratoří, kde zaměstnanci nakládají s nebezpečnými látkami. V případě zanedbání preventivních opatření (povinné nošení ochranného oděvu a obuvi, zákaz konzumace jídla a pití apod.) může zaměstnancům hrozit vážná újma na zdraví. Prostřednictvím kamerového systému proto zaměstnavatel (vedoucí zaměstnanec) sleduje, zda zaměstnanci dodržují pokyny v oblasti bezpečnosti a ochrany zdraví při práci po celou dobu svého pobytu v laboratoři. Zároveň je pořizován záznam snímaných prostor, který se automaticky vymaže na konci každého pracovního dne. Pokud však dojde k incidentu porušení bezpečnostních opatření, je záznam uchován po dobu jednoho týdne za účelem zajištění důkazního prostředku pro účely upozornění zaměstnance na porušení povinností vyplývajících z právních předpisů vztahujících se k jím vykonávané práci a na možnost výpovědi s tím související a též pro účely obrany zaměstnavatele v případě, že došlo k pracovnímu úrazu.

(c) Kamerový systém se záznamem uchovávaným po dobu několika dní

Zaměstnavatel v tomto scénáři provozuje zásilkovou službu. Do prostor skladu, kde zaměstnanci přijímají balíky od jednotlivých obchodů a vypravují je k odeslání koncovým zákazníkům, je nainstalován kamerový systém za účelem ochrany majetku a prevence a odhalování případných krádeží. Pořízené záznamy jsou uchovávány po dobu tří dnů pro případ, že zákazník po doručení zásilky reklamuje její obsah s tím, že

mu zásilka byla doručena rozbitá, nekompletní, případně očividně vykradená. Teprve v takovém případě zaměstnavatel prohlédne pořízený záznam za účelem zjištění, zda došlo k otevření balíku, nežádoucí manipulaci s ním nebo přímo ke krádeži. V případě potřeby je záznam uchován po dobu dvou týdnů pro účely upozornění příslušného zaměstnance na porušení povinností vyplývajících z právních předpisů vztahujících se k jím vykonávané práci, respektive požadování náhrady škody po tomto zaměstnanci. Pokud došlo ke krádeži, bude záznam předán příslušnému policejnímu orgánu. Pokud však k žádnému incidentu nedojde, záznam se automaticky smaže po uplynutí tří dnů (tj. 72 hodin) od jeho pořízení.

2.3.4 Relevantní rozhodovací praxe

(a) Evropský soud pro lidská práva

Otázkou oprávněnosti sledování zaměstnanců pomocí kamerového systému se Evropský soud pro lidská práva zabýval ve věci Karin Köpke proti Německu (rozsudek ze dne 5. října 2010). Tento případ je specifický tím, že v něm soud podpořil zaměstnavatele, přestože ten zaměstnance sledoval skrytě. Okolnosti a odůvodnění případu podrobně popisuji výše v kapitole 1.5.2(b).[184]

Dále v současné době před Evropským soudem pro lidská práva probíhá řízení ve věci stížnosti podané paní Antovićovou a panem Mirkovićem proti Černé Hoře. Oba jsou vyučujícími na univerzitě a napadli zavedení kamerového systému v posluchárnách, které prosadil děkan bez jejich souhlasu. Důvodem monitoringu měla být ochrana majetku a osob, zajištění bezpečnosti studentů a sledování výuky. Přístup k záznamům měl mít pouze děkan, přičemž tyto měly být uchovávány po dobu jednoho roku.[185] Ke dni odevzdání této práce však tento případ dosud nebyl rozhodnut.

[184] Rozsudek Evropského soudu pro lidská práva, stížnost č. 420/07, ze dne 5. října 2010, Věc Karin Köpke proti Německu.

[185] Stížnost č. 70838/13 podaná k Evropskému soudu pro lidská práva dne 25. října 2013, Věc Nevenka Antović a Jovan Mirković proti Černé Hoře.

(b) ÚOOÚ a soudy České republiky

ÚOOÚ se zaměřuje na kontrolu zákonnosti kamerových systémů poměrně často, a to nejen v rámci své pravidelné kontrolní činnosti, ale zejména na základě podaných podnětů. Níže uvádím ty nejzajímavější případy, přičemž řada z nich byla následně předmětem soudního přezkumu.

V roce 2008 provedl ÚOOÚ kontrolu u společnosti Evropský investiční holding a.s. (pro účely následujícího výkladu dále jen „zaměstnavatel"), která instalovala kamerový systém do prostor jí provozovaného hotelu Savoy.[186] Monitorováni tak byli hoteloví hosté i zaměstnanci hotelu. Účelem monitoringu měla být ochrana majetku zaměstnavatele a hotelových hostů, ochrana práv na ochranu života a zdraví zaměstnanců a hotelových hostů a ochrana pověsti zaměstnavatele. Zvláštní povahu své činnosti zaměstnavatel spatřoval v tom, že provoz pětihvězdičkového hotelu přináší zvýšené povinnosti co se ochrany práv zaměstnavatele i hotelových hostů týče.

Případ se dostal až k Nejvyššímu správnímu soudu. Ten vyslovil již výše citovaný závěr (viz kapitola 2.3.1 výše), a sice že k instalaci kamerových systémů, s ohledem na jejich povahu a zásah do osobní integrity osob, je možné přistoupit až tehdy, pokud už veškeré méně invazivní prostředky selhaly anebo by nebyly schopny naplnit vytyčený účel, který je sledován. Primárně má tedy zaměstnavatel používat k ochraně svých zájmů opatření, která nevyžadují pořizování obrazových záznamů, např. využívat pancéřové dveře proti vandalismu, instalovat automatické brány a kontrolní zařízení, společné poplachové systémy, lepší a silnější osvětlení ulic během noci apod. Soud též odmítl výše uvedenou argumentaci zaměstnavatele týkající se zvláštní povahy jeho činnosti; dle názoru soudu naopak k vysoké úrovni poskytovaných služeb patří i vysoký standard v oblasti ochrany soukromí hotelových hostů.

Co se monitoringu zaměstnanců týče, konstatoval Nejvyšší správní soud, že „*míra ochrany soukromí je u zaměstnance určována (limitována, omezována) tím, že provádí*

[186] Případ měl také politický kontext; kontrola v hotelu Savoy byla totiž provedena poté, co na veřejnost unikla videonahrávka zachycující schůzku kancléře prezidenta Jiřího Weigla a lobbisty Miroslava Šloufa v lednu 2008 před prezidentskými volbami. Viz SLONKOVÁ, Sabina, JUNEK, Adam. Tajná schůzka před volbou prezidenta: Exkluzivní záznam [online]. Publikováno dne 4. února 2008 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://zpravy.aktualne.cz/domaci/tajna-schuzka-pred-volbou-prezidenta-exkluzivni-zaznam/r~i:article:520359/?redirected=1508444541>.

závislou práci, která je vykonávána ve vztahu nadřízenosti zaměstnavatele a podřízenosti zaměstnance, jménem zaměstnavatele, podle pokynů zaměstnavatele a zaměstnanec ji pro zaměstnavatele vykonává osobně… Monitoring zaměstnance je možný pouze na základě předchozího oznámení a jen tam, kde je to nezbytné k ochraně zdraví osob nebo majetku zaměstnavatele. Monitoring musí být směřován na majetek zaměstnavatele, nikoliv na osobu zaměstnance (nasměrování kamer), a musí být prováděn na pracovišti, nikoliv na místech určených k hygieně nebo k odpočinku zaměstnance." V daném případě soud neshledal naplnění podmínek § 316 odst. 2 ZP. Též s ohledem na další okolnosti případu posoudil soud zavedený monitoring jako nepřípustný a neproporcionální, a to jak ve vztahu k hotelovým hostům, tak k zaměstnancům hotelu.[187]

V roce 2010 uložil ÚOOÚ společnosti JRC Czech a.s. (pro účely následujícího výkladu dále jen „zaměstnavatel") pokutu za to, že v období let 2005 až 2009 zpracovávala osobní údaje svých zaměstnanců prostřednictvím fotografií ze záznamů kamer umístěných ve 20 prodejnách v různých městech České republiky. Zaměstnavatel se po neúspěšně podaném rozkladu bránil žalobou u správního soudu s tím, že monitoroval pouze prostor, v němž docházelo k obchodní činnosti, konkrétně prodejní pulty. Nemohl proto zasahovat do soukromého a osobního života zaměstnanců, neboť východiskem pracovněprávních vztahů je plnění pracovních úkolů zaměstnanci. Pořízené kamerové záznamy byly uchovávány po dobu jednoho měsíce v počítačových jednotkách a následně po dobu jednoho roku na CD a DVD nosičích. Důvodem zavedení monitoringu měla být ochrana majetku zaměstnavatele a prevence krádeží (zaměstnanci se údajně dopouštěli krádeží drahých herních konzolí a poskytovali slevy na zboží neexistujícím zákazníkům) a také kontrola otevírací doby. Zaměstnavatel argumentoval tím, že kontrolní právo vyplývající z § 316 odst. 2 ZP lze za stanovených podmínek přiznat každému zaměstnavateli.

Městský soud v Praze však žalobu zamítl s tím, že zásah do soukromí zaměstnanců nebyl přiměřený. Kromě jiného konstatoval, že ke kontrole otevírací doby mohl zaměstnavatel využít mírnějších prostředků (např. čipové karty nebo kameru snímající výhradně prostor vstupu do prodejny) a co se ochrany majetku týče, nemohl kamerový

[187] Rozsudek Nejvyššího správního soudu sp. zn. 5 As 158/2012 ze dne 23. srpna 2013.

systém zamířený jen na prodejní pult pomoci ochránit před krádeží herní konzole, které se nacházely v jiné části prodejny. Pro kontrolu poskytování slev neexistujícím zákazníkům by byla dle názoru soudu postačující kamera snímající pouze prostor před prodejním pultem, a nikoli prostor za ním, v němž se po většinu pracovní doby zdržují zaměstnanci. Uchovávání záznamů po dobu jednoho roku výrazně překračuje požadavek nezbytnosti; navíc takto byly uchovávány všechny záznamy bez rozdílu, zda zaznamenaly krádež či nikoli. Hodnocením, zda zaměstnavatel splnil podmínky § 316 odst. 2 ZP, se však soud nezabýval.[188] Proti tomuto rozsudku zaměstnavatel nepodal kasační stížnost.

V roce 2013 provedl ÚOOÚ kontrolu u zaměstnavatele zabývajícího se zámečnickými pracemi a nástrojářstvím, který instaloval kamerový systém za účelem ochrany majetku, ochrany před krádežemi, ochrany před zneužíváním technických zařízení a ochrany před neoprávněným jednáním zaměstnanců. Důvodem byly předchozí negativní zkušenosti zaměstnavatele s krádežemi a neoprávněným používáním strojového zařízení ze strany zaměstnanců. V jednom z případů krádeže bylo totiž po předání věci Policii ČR zjištěno, že pachatelem byl zaměstnanec. Před instalací kamerového systému nabídl zaměstnavatel zaměstnancům ještě možnost zavedení společné hmotné odpovědnosti. Zaměstnanci se většinově přiklonili raději ke kamerovému systému, následně ovšem podali podnět k ÚOOÚ se zdůvodněním, že kamerový systém neslouží k ochraně majetku, nýbrž k jejich šikaně. Po zhodnocení parametrů kamerového systému (k pořízeným záznamům měli přístup pouze jednatelé zaměstnavatele a správce systému na úrovni administrátora, přístupy byly zabezpečeny přihlašovacím jménem, heslem a znalostí IP adresy a byly logovány, kamerový systém byl provozován v samostatné IT síti, atd.) nicméně ÚOOÚ došel k závěru, že kamerový systém je provozován v souladu se ZOOÚ i § 316 odst. 2 ZP a že k narušování soukromí zaměstnanců nedochází.[189]

Další případ, který ÚOOÚ řešil, byl záměr společnosti STUDENT AGENCY, k.s. (pro účely následujícího výkladu dále jen „zaměstnavatel“) instalovat vždy jednu stacionární kameru do přední části každého z jí provozovaných autobusů. Důvodem pro instalaci kamerového systému měla být ochrana majetku a zdraví zaměstnanců, zvýšení

[188] Rozsudek Městského soudu v Praze sp. zn. 8A 182/2010 ze dne 2. září 2014.

[189] ÚOOÚ: Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2013. Brno: Nakladatelství MU Brno, 2014, s. 26 – 29. ISBN 978-80-210-6700-4.

bezpečnosti cestujících a přepravy a také použití záznamů jako důkazního materiálu při případných dopravních nehodách a při řešení stížností cestujících. Kamerový systém měl pořizovat záznam, jenž měl být uchováván po dobu pěti dnů u vnitrostátních linek a po dobu devíti dnů u mezinárodních linek. Co se sledování zaměstnanců týče, argumentoval zaměstnavatel tím, že vzhledem k tomu, že jím zaměstnaný řidič při jedné jízdě odpovídá za životy a zdraví zhruba 60 přepravovaných osob a dalších účastníků silničního provozu, je tím u zaměstnavatele dán pro monitoring zaměstnanců závažný důvod spočívající ve zvláštní povaze činnosti dle § 316 odst. 2 ZP. Dle názoru zaměstnavatele nemůže provádění takové kontroly nepřiměřeně zasahovat do soukromí zaměstnanců, neboť je monitorován prostor kabiny řidiče, který není soukromým prostorem a je otevřený a může stejně tak být sledován např. cestujícími či z vnějšku autobusu. Navíc, cílem monitoringu nemá být sledování soukromých aktivit řidiče, ale plnění jeho pracovních povinností.

ÚOOÚ nicméně takové zpracování osobních údajů zaměstnanců nepovolil s tím, že (i) zpracování osobních údajů prostřednictvím záznamu z kamery mířící na řidiče a jeho bezprostřední okolí je nedůvodným a nepřiměřeným zásahem do soukromí tohoto zaměstnance, (ii) deklarované účely jsou dosažitelné i jinými prostředky (např. telefonování či odesílání sms zpráv řidičem za jízdy a jiné okolnosti případné dopravní nehody budou moci dosvědčit cestující) a (iii) s ohledem na skutečnost, že veškerá činnost personálu autobusu probíhá transparentně a je pozorovatelná cestujícími, jeví se přidaná hodnota pořízených záznamů jako minimální z hlediska přínosu pro zaměstnavatele vzhledem k deklarovaným účelům, ale jako maximální z hlediska zásahu do soukromí zaměstnanců. Kamerový systém je vzhledem k jeho podrobnosti, soustavnosti a možné zneužitelnosti kvalitativně zcela odlišným způsobem monitoringu než skutečnost, že je řidič po celou dobu jízdy pod dohledem cestujících. Dle názoru ÚOOÚ navíc nelze běžné provozování autobusové přepravy považovat za zvláštní povahu činnosti dle § 316 odst. 2 ZP.

Výše uvedené závěry ÚOOÚ potvrdil i předseda ÚOOÚ v rozhodnutí o rozkladu podaném zaměstnavatelem. Navíc konstatoval, že existuje řada jiných prostředků, jejichž vhodnou kombinací lze deklarovaného účelu dosáhnout; např. by zaměstnavatel mohl provádět namátkové kontroly, kdy by řidiči byli předem informováni, že může

k takovým kontrolám docházet, avšak nikdy by dopředu nevěděli, zda zrovna mezi jejich cestujícími není nějaký „kontrolor“, který jejich chování sleduje. V uvedeném případě monitoring zaměstnance probíhající po většinu jeho pracovní doby bez možnosti uchýlení se mimo záběr kamery představuje nepřiměřený zásah do soukromí tohoto zaměstnance.[190]

Zaměstnavatel proti rozhodnutí ÚOOÚ podal správní žalobu, kde argumentoval zejména tím, že jím stanovených účelů monitoringu nelze dosáhnout jinými prostředky než právě kamerovým systémem. Sledování prostoru kabiny řidiče ze strany cestujících je nespolehlivé, nesystematické a reálně neuskutečnitelné, cestující jsou anonymní a zpětně nebude možné je vyhledat za účelem podání svědectví. Městský soud v Praze však žalobu zamítl a zopakoval závěry ÚOOÚ. Také konstatoval, že nepřetržitým monitoringem ani některých deklarovaných účelů nelze dosáhnout; kamerový systém nepřispěje k ochraně zdraví zaměstnanců či zvýšení bezpečnosti cestujících, jelikož sám o sobě žádnému závadnému jednání nezabrání. Naopak, u některých osob může vytvořit tak velký a nezvladatelný stres, který by byl ve svém důsledku kontraproduktivní, neboť by mohl vést ke zcela opačnému než žalobcem zamýšlenému účelu ochrany majetku, zdraví, životů osob a bezpečnosti silničního provozu.[191] Proti rozhodnutí Městského soudu v Praze podal zaměstnavatel kasační stížnost k Nejvyššímu správnímu soudu; řízení je vedeno pod sp. zn. 10 As 245/2016 a v době odevzdání této práce stále pokračuje.

K této problematice se nezávisle na výše uvedeném případu vyjádřila též Pracovní skupina. Uvedla příklad, kdy přepravní společnost do všech svých vozů instaluje kameru snímající obraz i zvuk s cílem zlepšit způsob řízení vozidla zaměstnancem. V případě, že dojde k nenadálým událostem typu selhání brzd nebo náhlé vybočení ze směru jízdy, pořídí kamera záznam. Takový monitoring označila Pracovní skupina za nepřípustný, neboť nepřiměřeně zasahuje do soukromí zaměstnance. Zaměstnavatel má použít méně invazivní metody, např. instalovat do vozidel zařízení, které znemožní

[190] Rozhodnutí předsedy Úřadu pro ochranu osobních údajů, č. j. UOOU-00363/13-41 ze dne 24. dubna 2013.

[191] Rozsudek Městského soudu v Praze sp. zn. 5 A 107/2013 ze dne 18. října 2016.

užívání mobilního telefonu za jízdy, nebo přijmout jiná bezpečnostní opatření (např. nouzové brzdy či zařízení upozorňující zaměstnance na vybočení z jízdního pruhu).[192]

2.4 Monitoring pomocí GPS

2.4.1 Úvodní poznámky

Monitoring pohybu zaměstnanců pomocí GPS (z anglického *Global Positioning System*) si zpravidla přejí zavést zaměstnavatelé, kteří zaměstnancům za účelem výkonu práce svěří služební vozidlo. S rozšířením chytrých telefonů a s tím, jak často bývají v praxi zaměstnancům svěřovány k výkonu práce, se nicméně nabízí sledování polohy zaměstnanců i právě prostřednictvím těchto zařízení. Informace o tom, kde se zaměstnanec nachází, jakou použil při výkonu své práce trasu, zda dorazil na místo určení, na jakých místech a na jak dlouho se cestou zastavil, jak dlouho mu trvala cesta a jakou urazil vzdálenost apod., jsou osobními údaji ve smyslu definice obsažené v § 4 písm. a) ZOOÚ.[193] Nově jsou tyto tzv. lokační údaje výslovně definovány jako osobní údaje v čl. 4 odst. 1 GDPR. Technologie GPS umožní zaměstnavateli zpracovávat lokační údaje zaměstnance buď přímo (tj. pokud je sledován zaměstnanec jako takový např. pomocí zařízení připnutého k oblečení), nebo nepřímo (tj. pokud se sleduje poloha vozidla, mobilního telefonu či jiného zařízení, které bylo zaměstnanci svěřeno k užívání).[194]

Obvyklým důvodem pro zavedení monitoringu zaměstnance pomocí GPS zařízení instalovaného do vozidla, jenž za splnění testu proporcionality obstojí jako závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele dle § 316 odst. 2 ZP, bude ochrana majetku zaměstnavatele. Zejména v případě, kdy zaměstnavatel zaměstnancům nedovolí užívat svěřené vozidlo k soukromým účelům, umožní GPS poměrně efektivní kontrolu dodržování zákazu dle § 316 odst. 1 ZP. GPS však může zaměstnavateli sloužit

---

[192] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 21.

[193] RADIČOVÁ, Zuzana. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy*. 2014, roč. 22, č. 21, s. 737 – 738. ISSN 1210-6410.

[194] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko ohledně užívání lokačních údajů s přihlédnutím k poskytování služeb s přidanou hodnotou (v originále: „*Opinion on the use of location data with a view to providing value-added services*“) ze dne 25. listopadu 2005, s. 9.

i k další úspoře nákladů pomocí optimalizace tras, ke zlepšování přepravy v rámci navzájem vzdálených míst[195], případně ke kontrole dodržování dopravních předpisů nebo bezpečnostních přestávek po dosažení maximální doby řízení. Dalším důvodem pro zavedení monitoringu může být též zajištění bezpečnosti zaměstnance samotného nebo zboží, které bylo zaměstnanci k přepravě svěřeno (např. při rozvozu peněz do bankomatů, při převozu cenných kovů, šperků, apod.).[196] Bezpečí zaměstnance může být důvodem i pro zavedení GPS sledování prostřednictvím mobilního telefonu, např. pokud zaměstnanec pracuje v odlehlých či nebezpečných oblastech nebo v místech, kde není mobilní signál.

ÚOOÚ zastává názor, že sledování služebních vozidel je odůvodněné např. u kurýrních služeb nebo společností zajišťujících bezpečný převoz peněz.[197] Jak již v této práci zmiňuji několikrát, domnívám se, že závažný důvod spočívající ve zvláštní povaze vlastní činnosti obhájí i další „běžní" zaměstnavatelé. Za účelem kontroly dodržování zákazu užívání pracovních prostředků k soukromým účelům dle § 316 odst. 1 ZP může monitoring pomocí GPS z důvodu ochrany majetku zavést prakticky každý zaměstnavatel, který zaměstnanci svěří služební vozidlo.[198] Jak ovšem zdůrazňuje Pracovní skupina, sledování by bylo excesivní v případě, kdy by zaměstnanci byli oprávněni sami si organizovat cestu a cestování.[199]

Dodejme, že pokud by zaměstnavatel provedl pouze jednorázovou a namátkovou kontrolu zaměstnance pomocí GPS, případně tuto technologii využil pouze v omezeném časovém intervalu (např. za účelem jednorázové optimalizace trasy), nejednalo by se o sledování ve smyslu § 316 odst. 2 ZP.[200] V takovém případě by chyběl prvek systematičnosti a dlouhodobosti, který dané ustanovení dle mého názoru a dle části

---

195 Tamtéž, s. 10.

196 Tamtéž, s. 10.

197 ÚOOÚ: Ochrana osobních údajů na pracovišti. Příručka pro zaměstnance. Brno: Masarykova univerzita, 2014, s. 18. ISBN 978-80-210-6819-3.

198 Viz též MORÁVEK, Jakub. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy*. 2017, roč. 25, č. 17, s. 579. ISSN 1210-6410 (předpokladem tohoto závěru je nicméně dle Morávka skutečnost, že nebude za relevantní považován restriktivní výklad § 316 odst. 2 ZP.).

199 Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko ohledně užívání lokačních údajů s přihlédnutím k poskytování služeb s přidanou hodnotou (v originále: „*Opinion on the use of location data with a view to providing value-added services*") ze dne 25. listopadu 2005, s. 10.

200 RADIČOVÁ, Zuzana. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy*. 2014, roč. 22, č. 21, s. 737. ISSN 1210-6410.

literatury vyžaduje (viz též kapitolu 1.4). Zaměstnavatel by v takovém případě nemusel splnit podmínky a povinnosti stanovené v § 316 odst. 2 a 3 ZP.

2.4.2 Podmínky monitoringu

Jak doporučuje Výbor ministrů Rady Evropy, zaměstnavatelé by měli využívat zařízení umožňující sledování polohy zaměstnance pouze v případě, že k tomu mají skutečně legitimní důvod, jehož nelze dosáhnout jinak. Zároveň by užívání takových zařízení nemělo vést k nepřetržitému sledování zaměstnanců. Monitoring zaměstnance také nemá být hlavním cílem užívání technologie GPS, ale pouze nepřímým důsledkem přijetí kroků nezbytných k ochraně zaměstnavatelovy činnosti a jejího efektivního řízení nebo k zajištění bezpečnosti a ochrany zdraví při práci.[201]

Pokud zaměstnavatel instaluje GPS do vozidla nebo zařízení, které je zaměstnanec oprávněn užívat též k soukromým účelům, je povinen se vyvarovat sledování zaměstnance mimo pracovní dobu. Vozidla by proto měla být vybavena zařízením, které umožní přepínání z režimu služební jízdy do režimu soukromé jízdy a GPS by se měla po přepnutí do režimu soukromé jízdy zcela vypnout.[202] Pokud je GPS instalována v jiném zařízení (např. mobilní telefon či notebook), musí mít zaměstnanec také možnost ji po skončení pracovní doby vypnout. Jestliže zaměstnavatel zamýšlí pomocí technologie GPS chránit vozidlo nebo jiné zařízení proti krádeži, nebude se jednat o opatření sloužící ke sledování zaměstnance, a tak by s ním zaměstnavatelé měli zacházet. S ohledem na minimalizaci zásahů do soukromí zaměstnance by mělo takové opatření fungovat např. na principu zaslání upozornění zaměstnavateli v případě, že vozidlo opustí určitý předem vymezený prostor (např. určitý kraj, kde se má zaměstnanec během výkonu své práce zdržovat, území České republiky, apod.).[203]

---

[201] Výbor ministrů Rady Evropy: Doporučení Výboru ministrů členským státům č. CM/Rec(2015)5 ohledně zpracování osobních údajů v kontextu zaměstnání, čl. 16.

[202] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 20.

[203] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 13/2011 o geolokalizačních službách u inteligentních mobilních zařízení (v originále: „*Opinion 13/2011 on Geolocation services on smart mobile devices*“) ze dne 16. května 2011, s. 14.

Co se týče doby uchování osobních údajů shromážděných během sledování polohy zaměstnance, doporučuje Pracovní skupina, aby tato nepřesáhla dobu dvou měsíců. Pokud by si zaměstnavatel přál údaje uchovávat po delší dobu (např. pro účely dlouhodobé analýzy záznamů o ujetých trasách za účelem jejich optimalizace), měl by je předtím anonymizovat.[204]

2.4.3 Konkrétní příklady scénářů monitoringu pomocí GPS

(a) Sledování služebního vozidla zaměstnance, které lze zároveň užívat k soukromým účelům

Zaměstnavatel v tomto scénáři svěří služební vozidlo zaměstnanci, jehož hlavní náplní práce je provádění pravidelného servisu plynových kotlů instalovaných u zákazníků po celé České republice. Zároveň je zaměstnanec oprávněn svěřené vozidlo užívat pro soukromé účely. Za účelem ochrany majetku zaměstnavatele a optimalizace tras bylo do vozidla instalováno zařízení s technologií GPS. Zaměstnanec je seznámen s vnitropodnikovou směrnicí upravující podmínky užívání služebního vozidla včetně jeho sledování pomocí GPS a je výslovně upozorněn na povinnost přepínat mezi režimem služební a soukromé jízdy. Během režimu služební jízdy budou zaznamenávány údaje o poloze vozidla, ujeté trase, času stráveném jízdou a počtu ujetých kilometrů. Během režimu soukromé jízdy bude GPS zcela vypnuta. Zaznamenané údaje budou uchovávány po dobu jednoho měsíce a budou sloužit ke kontrole spotřebovaného paliva, vedení knihy jízd, optimalizaci tras a souvisejícímu plánování servisních kontrol u zákazníků.

(b) Sledování služebního vozidla užívaného pro dálkové trasy

Zaměstnavatel v tomto scénáři pravidelně vysílá zaměstnance na pracovní cestu do své pobočky v zahraničí, přičemž jim za účelem přepravy na místo určení vždy svěřuje služební vozidlo. Toto vozidlo nejsou zaměstnanci oprávněni užívat k soukromým účelům. Za účelem kontroly dodržování maximální povolené rychlosti a povinných

[204] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko ohledně užívání lokačních údajů s přihlédnutím k poskytování služeb s přidanou hodnotou (v originále: „*Opinion on the use of location data with a view to providing value-added services*“) ze dne 25. listopadu 2005, s. 10 – 11.

bezpečnostních přestávek stanovených příslušnými právními předpisy[205], jakož i kontroly dodržování zákazu užívání vozidla k soukromým účelům během pracovní cesty (např. k soukromým výletům po cestě apod.), instaluje zaměstnavatel do vozidla zařízení s aplikací GPS. S povinnostmi souvisejícími s řízením referentského vozidla, jakož i s okolnostmi monitoringu, je zaměstnanec předem seznámen prostřednictvím pravidelných školení a vnitropodnikové směrnice. Zaměstnavateli jsou odesílány údaje o počtu ujetých kilometrů, absolvované trase a času stráveném na cestě a dále o případech překročení maximální povolené rychlosti v úseku delším než 1 km a o porušení povinnosti zaměstnance čerpat bezpečnostní přestávku v souladu s právními předpisy. Zároveň GPS aplikace preventivně upozorňuje zaměstnance během jízdy na překročení maximální rychlosti povolené v daném úseku a na blížící se čas k čerpání povinné bezpečnostní přestávky. Shromážděné údaje zaměstnavatel uchovává po dobu 10 dnů, aby mohl z porušení povinností ze strany zaměstnance případně vyvodit důsledky.

(c) Sledování polohy zaměstnance prostřednictvím mobilního telefonu

Zaměstnavatel v tomto scénáři provozuje kurýrní službu po Praze s tím, že pro něj pracují kurýři užívající k výkonu své práce jízdní kolo. Za účelem optimalizace předávání a doručování zásilek a za účelem ochrany bezpečnosti a zdraví kurýra (pro případy dopravní nehody nebo napadení kurýra třetí osobou – při delší době nečinnosti je zaměstnanec kontaktován centrálou, zda je vše v pořádku) se zaměstnavatel rozhodne vybavit kurýry služebním mobilním telefonem, který pomocí aplikace GPS zachycuje jejich polohu v reálném čase. Po skončení pracovní doby jsou kurýři povinni mobilní telefon odevzdat a nejsou oprávněni jej využívat k soukromým účelům. Po dobu čerpání přestávky v práci na jídlo a oddech jsou kurýři povinni aplikaci GPS vypnout. Údaje pořízené pomocí GPS zaměstnavatel neuchovává, zaměstnanci jsou sledováni v režimu online.

[205] Bod 3. přílohy č. 1 k nařízení vlády č. 168/2002 Sb., kterým se stanoví způsob organizace práce a pracovních postupů, které je zaměstnavatel povinen zajistit při provozování dopravy dopravními prostředky, ve znění pozdějších předpisů.

2.4.4 Relevantní rozhodovací praxe

Rozhodovací praxe v oblasti sledování zaměstnanců pomocí technologie GPS není příliš rozsáhlá. Prozatím se této problematice nevěnoval ani Evropský soud pro lidská práva.

Známý je nicméně případ České pošty, s.p. (dále jen „zaměstnavatel“), která vybavila své zaměstnance, a to všechny listovní doručovatele pěší a listovní doručovatele motorizované v počtu nejméně 7770 osob, zařízením (tzv. tracerem) s technologií GPS. Účelem sledování zaměstnanců měla být kontrola a optimalizace doručovacích okrsků (sledování jejich vytíženosti, zajištění obslužnosti monitorovaného území, ochrana zaměstnanců před nerovnoměrnou vytížeností apod.) a využití zaznamenaných údajů při vyřizování případných reklamací. Zpracovávány byly údaje o délce trasy a času stráveném na trase. Rovněž bylo prováděno vyhodnocení, zda se doručovatel pohyboval pouze ve svém okrsku, byla pořizována evidence a zobrazovány události označené doručovatelem v průběhu pochůzky, vyhotovováno procentuální vyjádření obslužnosti doručovacího okrsku (poměr navštívených doručovacích míst vůči celkovému počtu doručovacích míst), identifikována doručovací místa s největším počtem návštěv a pořizován kompletní rozpis navštívených/nenavštívených doručovacích míst. Pohyb zaměstnanců nebyl sledován v reálném čase, ale teprve po skončení pracovní doby byl pořizován zpětně zobrazitelný záznam o jejich pohybu ukládaný v anonymizované podobě. Zaměstnanci byli oprávněni sledovací zařízení vypnout během čerpání přestávky v práci na jídlo a oddech. Údaje byly systematicky shromažďovány téměř po dobu celého jednoho roku. Sledovací systém však nezaznamenával jméno a příjmení konkrétního doručovatele, a zaměstnavatel proto tvrdil, že pomocí technologie GPS byla zpracovávána pouze statistická data bez jakékoli vazby na jednotlivé zaměstnance. Propojit shromážděné informace s konkrétním zaměstnancem nicméně bylo možné pomocí jejich porovnání s rozpisem služeb doručovatelů na příslušné poště, na což při kontrole poukázal ÚOOÚ.

Dle názoru ÚOOÚ neodpovídal rozsah zpracovávaných údajů účelům využití technologie GPS, neboť byl nepřiměřený. K optimalizaci doručovacích okrsků by postačoval monitoring prováděný pouze po několik dnů s následným vyhodnocením výsledků. Pro účely vyřizování případných reklamací a zajištění kvality poskytovaných poštovních služeb by bylo dostatečné shromažďovat a vyhodnocovat pouze údaje

o navštívených doručovacích místech v rozsahu místo a čas. ÚOOÚ ani neuznal argumentaci zaměstnavatele, že doručování poštovních zásilek (dle zaměstnavatele služba poskytovaná ve veřejném zájmu) představuje závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele dle § 316 odst. 2 ZP. Za nepřiměřený monitoring zaměstnanců byla proto zaměstnavateli uložena pokuta ve výši 80 000 Kč.[206]

Proti rozhodnutí ÚOOÚ zaměstnavatel neúspěšně podal rozklad; následně se obrátil se správní žalobou k soudu. Městský soud v Praze se však ztotožnil se závěry ÚOOÚ a žalobu zamítl. Konstatoval, že povahu činnosti zaměstnavatele nelze považovat za natolik zvláštní, aby mohla odůvodňovat narušení soukromí doručovatelů při pochůzce na trase v příslušném doručovacím okrsku. Povinnost plnit podmínky poštovní licence a zákona[207] nečiní z činnosti zaměstnavatele takovou činnost, která by odůvodňovala nerespektování soukromí zaměstnanců na pracovišti. Navíc, využití technologie GPS nemohlo zabránit případnému nedoručení zásilek jejich adresátům, ani takové pochybení zaměstnance zachytit. Shodně s ÚOOÚ, který došel k závěru, že „*doručovatelé neměli při výkonu své práce jakékoli soukromí, neboť byl monitorován každý jejich pohyb, a byli tak pod neustálým dozorem a nemohli si ani zajít do obchodu koupit svačinu, aniž by o tom zaměstnavatel měl záznam*“, tak soud konstatoval, že zpracování osobních údajů zaměstnanců pomocí technologie GPS nebylo v tomto případě přiměřené.[208] Proti rozhodnutí Městského soudu v Praze nicméně zaměstnavatel nepodal kasační stížnost.

2.5 Monitoring užívání služebních telefonů

2.5.1 Úvodní poznámky

Řada zaměstnavatelů si především s ohledem na kontrolu vynaložených nákladů přeje mít přehled o užívání pevných linek ze strany svých zaměstnanců a zejména mobilních telefonů, které svým zaměstnancům za účelem výkonu práce svěřují. Předně je třeba

[206] Rozhodnutí Úřadu pro ochranu osobních údajů, č. j. UOOU-00237/13-38 ze dne 3. července 2013.

[207] Zákon č. 29/2000 Sb., o poštovních službách, ve znění pozdějších předpisů.

[208] Rozsudek Městského soudu v Praze sp. zn. 6 A 42/2013 ze dne 5. května 2017.

připomenout, že čl. 13 Listiny základních práv a svobod zaručuje tajemství zpráv podávaných telefonem ve stejném rozsahu, v jakém je chráněno listovní tajemství. V již výše citovaném nálezu (viz kapitolu 2.1.1) Ústavní soud nicméně konstatoval, že tajemství zpráv podávaných telefonem nelze vztahovat na činnost, která má být svou povahou činností pracovní.[209] I toto základní právo tak lze při splnění testu proporcionality omezit ve prospěch práv zaměstnavatele.

Jako závažný důvod ve smyslu § 316 odst. 2 ZP obstojí pro kontrolu užívání služebního telefonu ochrana majetku zaměstnavatele, a to zejména v případě, kdy zaměstnavatel zaměstnancům nedovolí užívání služebního telefonu pro soukromé účely, nebo toto užívání dovolí, ale v omezeném rozsahu. Co se týče možnosti pořizování záznamů telefonických hovorů uskutečněných zaměstnancem jménem zaměstnavatele, ÚOOÚ ve svém stanovisku zmiňuje pouze dva legitimní důvody ospravedlňující takovou praxi. Prvním z nich je případ, kdy mají zaměstnanci prostřednictvím telefonu kontaktovat stávající či potenciální zákazníky zaměstnavatele, který tyto hovory nahrává, neboť potřebuje mít jejich obsah k dispozici pro účely plnění smlouvy nebo pro jednání o uzavření nebo změně smlouvy.[210] Druhý případ představuje nahrávání telefonických hovorů zaměstnanců s klienty zaměstnavatele za účelem zvyšování kvality poskytovaných služeb, s čímž souvisí kontrola práce zaměstnanců. V těchto případech dle ÚOOÚ zásah do soukromí zaměstnanců nebude převažovat nad právem zaměstnavatele na ochranu jeho práv, případně práv a právem chráněných zájmů jeho klientů, samozřejmě při splnění dalších požadavků vyplývajících z příslušné právní úpravy.[211]

Kontrola užívání telefonu, stejně jako pořizování nahrávek hovorů, bude představovat zpracování osobních údajů; o to by se nejednalo pouze v případě živých odposlechů bez pořizování jejich nahrávek.

S ohledem na ochranu danou Listinou základních práv a svobod nebude zaměstnavatel nikdy oprávněn odposlouchávat a/nebo pořizovat záznam soukromých telefonických

[209] Usnesení Ústavního soudu sp. zn. I. ÚS 452/09 ze dne 31. března 2009.

[210] Ve vztahu k zákazníkům tak bude využita výjimka pro zpracování jejich osobních údajů bez jejich souhlasu dle § 5 odst. 2 písm. b) ZOOÚ, respektive čl. 6 odst. 1 písm. b) GDPR.

[211] ÚOOÚ: Stanovisko č. 5/2013: Pořizování hlasových záznamů v rámci elektronické komunikace při poskytování služeb z pohledu zákona o ochraně osobních údajů. Říjen 2013, s. 2 – 3.

hovorů, i kdyby je zaměstnavatel učinil z telefonu zaměstnavatele, na pracovišti a v pracovní době.[212] Jak konstatoval Nejvyšší soud, zaměstnavatel je povinen respektovat tajemství zpráv dopravovaných jeho telekomunikačním zařízením i v případě, kdy toto zařízení použil zaměstnanec k účelům nesouvisejícím s plněním jeho pracovních úkolů. To samozřejmě zaměstnavatele nezbavuje práva na náhradu škody, která mu zneužitím jeho telekomunikačního zařízení vznikla, a to podle příslušných ustanovení pracovněprávních předpisů (tento případ je podrobněji rozebrán v kapitole 2.5.4(b) níže).[213]

2.5.2 Podmínky monitoringu a jeho základní způsoby

Pokud jde o sledování užívání telefonu za účelem ochrany majetku zaměstnavatele, je zaměstnavatel oprávněn tak činit v rozsahu údaj o volaném telefonním číslu, datum, čas a délka hovoru.[214] Samozřejmě pouze z těchto údajů nelze a priori dovodit, zda se jednalo o soukromý nebo pracovní telefonát.[215] Zaměstnavatel nicméně může zaměstnance konfrontovat a požadovat vysvětlení ke konkrétním volaným telefonním číslům (zpravidla u často volaných čísel, u hovorů, které trvaly déle než ostatní, u hovorů do zahraničí apod.).

Umožní-li zaměstnavatel zaměstnancům užívat telefon též pro soukromé účely, ať už neomezeně, nebo v určitém předem omezeném rozsahu (respektive mimo pracovní dobu nebo v přiměřeném rozsahu též v pracovní době), měl by podrobná pravidla nastavit ve vnitřním předpise a zaměstnance informovat, jakým způsobem bude užívání telefonu kontrolováno, případně zda budou zaměstnanci povinni za tyto soukromé hovory platit. Zaměstnanci tak mohou mít povinnost každý soukromý hovor předem stanoveným způsobem označit, např. předvolbou „*“ (hvězdička) před vytáčeným telefonním číslem. To může usnadnit následnou fakturaci v případě, že jsou

---

[212] JOUZA, Ladislav. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. *Bulletin advokacie*. 2014, č. 6, s. 29. ISSN 1210-6348.

[213] Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1009/98 ze dne 21. října 1998.

[214] KADLECOVÁ, Tereza. Monitoring zaměstnanců. *Praktická personalistika*. 2015, roč. 3, č. 11 – 12, s. 26. ISSN 2336-5072.

[215] JOUZA, Ladislav. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. *Bulletin advokacie*. 2014, č. 6, s. 29. ISSN 1210-6348.

zaměstnanci povinni za tyto soukromé hovory zaměstnavateli platit prostřednictvím srážek ze mzdy.[216] Další pravidla stanovená vnitřním předpisem mohou zahrnovat určení paušální částky, kterou jsou zaměstnanci oprávněni provolat pro svou soukromou potřebu, zákaz volání na zahraniční čísla bez předchozího schválení vedoucího zaměstnance, zákaz volání ze zahraničí, apod. Zaměstnavatel by měl ve vnitřním předpise pamatovat též na SMS zprávy. Řada velkých zaměstnavatelů nicméně přechází na neomezené tarify, kde pochopitelně odpadá smysl rozlišovat mezi soukromými a pracovními hovory, co se vynaložených nákladů týče. Zde může mít smysl sledovat (a případně též postihovat), zda si zaměstnanci vyřizují soukromé telefonáty v pracovní době.

Co se týče pořizování nahrávek telefonních hovorů zaměstnanců se zákazníky pro účely zvyšování kvality služeb poskytovaných zaměstnavatelem, upozorňuje ÚOOÚ, že by nebylo přiměřené nahrávat všechny hovory zaměstnance. Pro daný účel postačí nahrávat pouze vybraný vzorek telefonátů, které budou následně ze strany zaměstnavatele vyhodnocovány. Zaměstnavatel by měl stanovit určitá pravidla, jak budou hovory nahrávány (např. nejvýše dva hovory denně), a při jejich vyhodnocování by měl zaměstnanci umožnit se k pořízeným nahrávkám vyjádřit. Co se týče délky uchovávání záznamů pro účely zvyšování kvality služeb, postačí dle ÚOOÚ cca jeden měsíc, během něhož by měly být vyhodnoceny a následně zlikvidovány. Delší doba uchování bude přípustná tehdy, pokud budou nahrávky nezbytné též pro účely plnění smlouvy se zákazníkem.[217]

Zajímavé je, že se k problematice sledování užívání telefonů a/nebo nahrávání hovorů zaměstnanců specificky nevyjadřuje Pracovní skupina. To je s ohledem na tento relativně častý způsob zpracování osobních údajů neobvyklé.

---

[216] BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi*. 2. vyd. Praha: LINDE, 2010, s. 148. ISBN 978-80-7201-817-8.

[217] ÚOOÚ: Stanovisko č. 5/2013: Pořizování hlasových záznamů v rámci elektronické komunikace při poskytování služeb z pohledu zákona o ochraně osobních údajů. Říjen 2013, s. 3 – 4.

2.5.3 Konkrétní příklady scénářů monitoringu

(a) Možnost omezeného užívání mobilního telefonu pro soukromé účely

Zaměstnavatel svěří zaměstnancům za účelem výkonu práce mobilní telefon se zvýhodněným tarifem s tím, že jim umožní jej užívat mimo pracovní dobu též pro soukromé účely. Zároveň určí maximální částku, kterou mohou zaměstnanci měsíčně provolat (či využít pro zasílání SMS zpráv) bez ohledu na skutečnost, zda se bude jednat o pracovní či soukromé hovory. Pokud provolají více, je jim předložen výpis volaných čísel s tím, že jsou povinni označit, zda se jedná o soukromý či pracovní hovor, přičemž u pracovních hovorů musejí uvést konkrétní volanou osobu (jméno klienta). Náklady na soukromé hovory v rozsahu přesahujícím paušální částku pak musejí zaměstnavateli uhradit. Zároveň, zjistí-li zaměstnavatel, že zaměstnanec volal pro svou soukromou potřebu v pracovní době, může z toho v závislosti na množství takto provolaného času vyvodit další pracovněprávní důsledky (např. upozornění zaměstnance na možnost výpovědi nebo přímo výpověď pro závažné porušování povinností vyplývajících z právních předpisů vztahujících se k jím vykonávané práci).

(b) Nahrávání hovorů v call centru

Zaměstnavatel, telefonní operátor, provozuje call centrum, jehož zaměstnanci mají za úkol telefonicky kontaktovat stávající zákazníky zaměstnavatele a nabízet jim změnu tarifu. Za účelem plnění smluvních povinností jsou veškeré hovory se zákazníky nahrávány. Zároveň je každý den vždy jeden z nahraných hovorů vyhodnocován ze strany zaměstnavatele za účelem kontroly vystupování zaměstnance vůči zákazníkovi (a souvisejícího zvyšování kvality poskytovaných služeb). Objedná-li si zákazník změnu tarifu, je nahrávka uchovávána do okamžiku, kdy zákazníci podepíší písemnou smlouvu o změně tarifu. Pokud si zákazník změnu tarifu neobjedná, nahrávka je smazána na konci pracovního dne, ledaže byla vybrána pro účely vyhodnocování jednání zaměstnanců. V takovém případě je uchována po dobu dvou týdnů, během nichž je vyhodnocena a s výsledkem tohoto vyhodnocení je zaměstnanec seznámen.

2.5.4 Relevantní rozhodovací praxe

(a) Evropský soud pro lidská práva

Kontrolou užívání pracovního telefonu zaměstnancem se Evropský soud pro lidská práva zabýval ve věci Halfordová proti Spojenému království (rozsudek ze dne 25. června 1997) a ve věci Coplandová proti Spojenému království (rozsudek ze dne 3. dubna 2007).

Paní Halfordová, policistka, se neúspěšně ucházela o vyšší pracovní pozici, přičemž se domnívala, že hlavním důvodem jejího neúspěchu je skutečnost, že je ženou. Dala proto podnět k zahájení řízení o diskriminaci na základě pohlaví. Následně zaměstnavatel údajně zahájil odposlechy jejích telefonů, dle paní Halfordové proto, aby proti ní mohl takto zjištěné informace použít v řízení o diskriminaci. Zaměstnavatel přitom paní Halfordové svěřil dva telefony, z nichž jeden měla doma a byla oprávněna jej užívat pro soukromé účely a druhý měla ve své kanceláři; zároveň nebyla určena žádná bližší pravidla užívání těchto telefonů. Oba telefony byly součástí interní policejní telefonní sítě, která nespadala do veřejné telekomunikační sítě, a oba měly být zaměstnavatelem odposlouchávány, a to bez vědomí paní Halfordové. Soud dospěl k závěru, že telefonická komunikace, bez ohledu na skutečnost, zda byla učiněná z domova nebo z kanceláře, požívá ochrany dle čl. 8 Úmluvy o ochraně lidských práv a základních svobod. Paní Halfordová proto mohla rozumně předpokládat, že soukromí jejích hovorů je zachováno, přičemž toto rozumné očekávání zesilovaly další faktory, např. výslovně deklarovaná možnost užívat domácí telefon pro soukromé účely a kancelářský telefon pro účely komunikace v rámci řízení o diskriminaci. Soud došel k závěru, že odposlech telefonu v kanceláři paní Halfordové představoval zásah do jejího soukromí garantovaného čl. 8 Úmluvy o ochraně lidských práv a základních svobod. Pro úplnost dodejme, že odposlouchávání domácího telefonu nebylo prokázáno.[218]

Okolnosti případu paní Coplandové a závěry soudu jsou podrobně rozebrány již v kapitole 2.1.4(a) výše. V rámci (skryté) kontroly, zda paní Coplandová nadměrně neužívá telefon zaměstnavatele pro svou soukromou potřebu, byla sledována podrobná vyúčtování týkající se jejího pracovního telefonu, a to v rozsahu volaných telefonních

[218] Rozsudek Evropského soudu pro lidská práva, stížnost č. 20605/92, ze dne 25. června 1997, Věc Halfordová proti Spojenému království.

čísel, data, času, délky a ceny jednotlivých hovorů. Zaměstnavatel tvrdil, že toto sledování trvalo po několik měsíců, zatímco paní Coplandová tvrdila, že muselo trvat nejméně 18 měsíců a že musely být takto sledovány též její příchozí hovory. Jednotlivé telefonáty nebyly nahrávány. Soud konstatoval, že sledování údajů o telefonátech (zejména o volaných číslech) představuje zásah do soukromí zaměstnance, v daném případě navíc nezpochybnitelný tím, že jej zaměstnavatel prováděl skrytě.[219]

(b) ÚOOÚ a soudy České republiky

Rozhodovací praxe českých orgánů není v oblasti sledování užívání pracovního telefonu ze strany zaměstnanců, respektive pořizování nahrávek hovorů, příliš bohatá. Relevantní jsou nicméně následující rozsudky Nejvyššího soudu vydané v souvislosti s posuzování neplatnosti rozvázání pracovního poměru se zaměstnancem.

Na prvním místě uveďme rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1009/98 ze dne 21. října 1998. Zaměstnavatel okamžitě zrušil pracovní poměr se zaměstnancem z důvodu zvlášť hrubého porušení pracovní kázně spočívajícího v „*přípravě převzetí obchodů společnosti na vlastní účet, tudíž sabotování jednání ve prospěch společnosti, záměru snížení obratu společnosti, obcházení svých vedoucích pracovníků ve spojení se zahraničním partnerem a jejich znevažování způsobem, který je v zásadním rozporu s etikou v těchto vztazích*.“ Toto údajné jednání zaměstnance chtěl zaměstnavatel prokázat prostřednictvím nahrávek telefonických hovorů zaměstnance s jistou třetí osobou, jež ovšem byly pořízeny bez jejich vědomí. Soudy nižších stupňů však takový důkaz neprovedly (soud prvního stupně z důvodu nadbytečnosti takového důkazu pro dané řízení, odvolací soud z důvodu nepřípustnosti takového důkazu) a okamžité zrušení pracovního poměru posoudily jako neplatné. Zaměstnavatel podal dovolání s tím, že dle jeho názoru je použití důkazu záznamem telefonických rozhovorů mezi zaměstnanci přípustné. Zaměstnavatel je přece oprávněn monitorovat telefonické hovory svých zaměstnanců, aby mohl chránit svá práva a práva ostatních zaměstnanců. Skutečnost, že zaměstnanci hovoří z aparátů v jeho majetku (a navíc tento hovor zaplatil) podle názoru zaměstnavatele omezuje práva na ochranu přepravovaných zpráv zaměstnance ve prospěch ústavního práva zaměstnavatele na ochranu vlastnictví.

[219] Rozsudek Evropského soudu pro lidská práva, stížnost č. 62617/00, ze dne 3. dubna 2007, Věc Coplandová proti Spojenému království.

Zaměstnavatel se domníval, že zpráva uskutečněná za uvedených podmínek je vlastnictvím zaměstnavatele, který s ní může volně nakládat a může ji použít v rámci pracovněprávního sporu, jinak by se jednalo o nucené omezení vlastnických práv zaměstnavatele.

Nejvyšší soud však konstatoval, že „*zprávami podávanými telefonem ve smyslu čl. 13 Listiny a korespondencí ve smyslu čl. 8 odst. 1 Evropské úmluvy mohou být i zprávy komunikované zaměstnancem v telefonickém hovoru jinému zaměstnanci prostřednictvím telekomunikačního zařízení jejich zaměstnavatele. Zaměstnavatel není oprávněn takové telefonické hovory bez souhlasu hovořících zaměstnanců či alespoň jejich předchozího upozornění odposlouchávat nebo - jak uvádí dovolatelka - „monitorovat“, a to ani v případě, že zprávy v těchto hovorech podávané se týkají jeho zájmů*“. Za nesprávnou označil soud též domněnku zaměstnavatele, že z jeho vlastnického práva k telekomunikačnímu zařízení vyplývá i jeho vlastnictví ke zprávám, které jsou prostřednictvím tohoto zařízení podávány. Zprávy dopravované telefonem nelze považovat za majetek, který by mohl být předmětem vlastnického práva, a zákaz se s těmito zprávami seznamovat nemůže představovat nucené omezení tohoto práva. Důkaz záznamem telefonických hovorů, jenž byl pořízen bez vědomí těchto osob, proto soud označil za nepřípustný a dovolání zamítl.[220] Ačkoli soud rozhodoval dle předchozí právní úpravy, jsou dle mého názoru jeho závěry použitelné i dnes.

Dalším relevantním rozhodnutím je rozsudek Nejvyššího soudu sp. zn. 21 Cdo 747/2013 ze dne 7. srpna 2014; okolnosti případu i závěry soudu jsou již popsány v kapitole 2.2.4(b), neboť monitorováno bylo více aktivit než jen užívání služebního telefonu. Zaměstnanec v pracovní době ve dnech 20. ledna až 19. února 2010 zneužil přidělený firemní telefon pro soukromé účely, a to pro celkem 84 hovorů. Zaměstnanec v žalobě na neplatnost výpovědi z pracovního poměru argumentoval tím, že zaměstnavatel nesplnil podmínky § 316 odst. 2 ZP. Nejvyšší soud však konstatoval, že toto ustanovení se vůbec neuplatní, neboť zaměstnavatel nezjišťoval obsah telefonátů, ale pouze skutečnost, zda zaměstnanec respektoval zákaz užívání

[220] Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1009/98 ze dne 21. října 1998.

zaměstnavatelových pracovních prostředků pro soukromé potřeby dle § 316 odst. 1 ZP.[221]

2.6 Další vybrané způsoby monitoringu zaměstnanců

Kromě výše uvedených nejčastějších způsobů monitoringu pochopitelně existuje celá řada dalších sledovacích opatření zaváděných zaměstnavateli. Některá z nich uvádím v této kapitole.

2.6.1 Monitoring docházky a vstupů do zabezpečených prostor pomocí biometrických údajů

S technologickým rozvojem začínají být poměrně běžně dostupné technologie čtení otisků prstů, rozpoznávání duhovky či celého obličeje, s nimiž dnes umí pracovat každý pokročilejší smartphone. Dá se proto očekávat, že čím dál více zaměstnavatelů bude chtít tyto biometrické údaje také využívat, např. pro sledování docházky zaměstnanců či ke kontrole jejich vstupu do zabezpečených prostor. Zatímco běžné elektronické docházkové a přístupové systémy lze relativně snadno obcházet (např. identifikační kartu zaměstnance použije jiný zaměstnanec nebo dokonce třetí osoba), biometriku obelstít nelze.

Biometrické údaje představují dle Pracovní skupiny velmi specifickou skupinu údajů, neboť jsou nejen informací o určitém subjektu, ale mohou sloužit k propojení jiných dostupných informací s určitou osobou, tj. sloužit jako jedinečné identifikátory. Typickými biometrickými údaji jsou otisky prstů, struktura sítnice, struktura obličeje či hlas, geometrie ruky, struktura žil, ale také hluboce zakořeněné dovednosti nebo charakteristický způsob chování (např. vlastnoruční podpis, úhozy na klávesnici, způsob chůze či mluvy apod.).[222] Využívání takových údajů by proto mělo být s ohledem na možné důsledky jejich zneužití velmi omezené.

---

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

[222] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 4/2007 k pojmu osobních údajů (v originále: „*Opinion 4/2007 on the concept of personal data*“) ze dne 20. června 2007, s. 8.

Pracovní skupina při výkladu Směrnice 95/46/ES připouštěla využívání biometrických údajů ze strany zaměstnavatelů, např. snímání otisků prstů a duhovky, k identifikaci zaměstnanců vstupujících do nebezpečných prostor určených pouze pro speciálně vyškolený personál (např. laboratoř, kde zaměstnanci pracují s nebezpečnými viry). Podmínkou takového využití je samozřejmě splnění testu proporcionality a nemožnost použít pro daný účel méně invazivní prostředky kontroly.[223] Dle § 4 písm. b) ZOOÚ jsou biometrické údaje výslovně označeny za citlivé údaje (nad rámec Směrnice 95/46/ES, která je sem neřadí), jež lze zpracovávat pouze za podmínek stanovených § 9 ZOOÚ. K této problematice vydal ÚOOÚ stanovisko, v němž popisoval podmínky, za nichž byli zaměstnavatelé oprávněni biometrické údaje využívat. S odvoláním na výše citované stanovisko Pracovní skupiny ÚOOÚ dospěl k závěru, že pokud budou biometrické údaje pomocí určitých postupů (tzv. hashování) převedeny na tzv. biometrickou šablonu (tj. redukovanou formu biometrických údajů), kterou nebude možné převést zpět na biometrické údaje, nebude zpracovávání těchto šablon představovat zpracování citlivých údajů. Zaměstnavatel by tak mohl tyto biometrické šablony zpracovávat jako běžné osobní údaje, tj. též pro ochranu práv a právem chráněných zájmů svých nebo jiné dotčené osoby. Při splnění testu proporcionality a dalších podmínek stanovených ZOOÚ by je proto dle ÚOOÚ mohl využívat i k evidenci docházky zaměstnanců.[224] Užívání přímo biometrických údajů jako takových pro běžnou evidenci docházky by bylo dle názoru ÚOOÚ zcela nepřiměřené.[225]

Situaci však značně mění GDPR, na což upozorňuje na svých internetových stránkách též ÚOOÚ.[226] Dle čl. 9 odst. 1 GDPR patří biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby do zvláštní kategorie osobních údajů, které lze zpracovávat pouze v případech stanovených v odst. 2 téhož článku. Jediná výjimka, o níž by mohl zaměstnavatel ze znění tohoto článku uvažovat, je zpracování na základě

---

[223] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 3/2012 o pokrocích v oblasti biometrických technologií (v originále: „*Opinion 3/2012 on developments in biometric technologies*“) ze dne 27. dubna 2012, s. 13.

[224] ÚOOÚ: Stanovisko č. 3/2009: Biometrická identifikace nebo autentizace zaměstnanců. Květen 2009.

[225] ÚOOÚ: Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2007, s. 42 – 43.

[226] ÚOOÚ: Změna v hodnocení úrovně právní ochrany biometrických údajů [online]. Publikováno 8. června 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/zmena-v-nbsp-hodnoceni-urovne-pravni-ochrany-biometrickych-udaju/d-23850>.

výslovného souhlasu příslušných zaměstnanců. Získávání souhlasu zaměstnanců se zpracováním osobních údajů v pracovněprávních vztazích však GDPR prakticky vylučuje (podrobný výklad viz v kapitole 1.5.2(a) výše). Jak upozorňuje ÚOOÚ, postup popsaný ve výše citovaném stanovisku využívající biometrické šablony již nadále nebude možný, neboť GDPR považuje i tyto šablony za zvláštní kategorii údajů. ÚOOÚ proto slibuje vydání aktualizovaného stanoviska na toto téma. To však v době odevzdání této práce stále nebylo dostupné.[227]

2.6.2 Monitoring užívání služebního počítače a práce se soubory

Zaměstnavatelé, kteří zaměstnancům neumožní používat svěřený služební počítač k soukromým účelům, si pochopitelně nepřejí, aby zaměstnanci na pevný disk v tomto počítači ukládali soukromé soubory (hudbu, fotografie, filmy, apod.) či do počítače instalovali aplikace a programy, které k výkonu práce nepotřebují (hry, přehrávače médií, apod.) a které by dokonce mohly být nelegální. Řada zaměstnavatelů si také přeje mít pod kontrolou, jaké dokumenty si zaměstnanci stahují z interní zaměstnavatelovy databáze do svého počítače, případně zda je dále ukládají na soukromá přenosná paměťová zařízení (flashdisky, externí pevné disky apod.).

Jako závažný důvod ve smyslu § 316 odst. 2 ZP ospravedlňující zavádění opatření sledujících užívání služebního počítače a práce se soubory ze strany zaměstnanců dle mého názoru obstojí ochrana majetku zaměstnavatele, ochrana utajovaných skutečností, bankovního nebo obchodního tajemství, jakož i ochrana důvěrných informací a know-how. Ve vnitropodnikové směrnici by měl zaměstnavatel specifikovat, zda jsou zaměstnanci oprávněni v počítači uchovávat soukromé soubory, respektive jakým způsobem (např. ve složce označené jako „soukromá“), za jakých okolností, případně zda vůbec, jsou zaměstnanci oprávněni stahovat dokumenty z databáze zaměstnavatele, zejména pokud mohou s dokumenty pracovat přímo v této databázi, aniž by je pro svou práci museli ukládat do počítače, a zda jsou oprávněni tyto dokumenty ukládat na vlastní externí paměťová zařízení.

[227] Tamtéž.

Před zavedením sledovacích opatření by měl zaměstnavatel upřednostnit prevenci před detekcí (jak obecně požaduje Pracovní skupina)[228] a zvážit postup pomocí zablokování možnosti užívat vlastní přenosná paměťová zařízení a samostatně instalovat programy a aplikace. U nejcitlivějších dokumentů lze jistě znemožnit jejich ukládání na pevný disk služebního počítače. Pro menší zaměstnavatele by však taková opatření mohla znamenat nutnost vynaložit nemalé náklady, a v jejich případě proto lze ospravedlnit pravidelnou kontrolu dodržování předem stanovených pravidel. Tu bude zpravidla provádět správce sítě prostřednictvím vzdáleného přístupu k počítači a/nebo softwaru monitorujícího pohyb souborů z interní databáze na jednotlivé počítače a z počítače na externí paměťová zařízení. Takový monitoring bude samozřejmě představovat zpracování osobních údajů.

V současné době řeší Evropský soud pro lidská práva stížnost zaměstnance, pana Liberta, jehož zaměstnavatel v jeho nepřítomnosti otevřel složku s dokumenty nazvanou „osobní data“. Tu měl zaměstnanec uloženou na pevném disku svého pracovního počítače. Údajně na základě takto zjištěných skutečností byl následně pan Libert propuštěn.[229] Ke dni odevzdání této práce však tento případ dosud nebyl rozhodnut.

2.6.3 Monitoring tiskových úloh

Především s ohledem na úsporu nákladů si zaměstnavatelé mohou přát mít přehled o využívání tiskáren a kopírovacích strojů a bránit zneužívání těchto zařízení k soukromým potřebám zaměstnanců. Podrobnosti ohledně možností užívání těchto zařízení a souvisejícího monitoringu by měla stanovit vnitropodniková směrnice. Závažným důvodem dle § 316 odst. 2 ZP opravňujícím zavedení monitoringu bude v tomto případě ochrana majetku zaměstnavatele.

Zaměstnanci tak mohou být např. povinni před každým tiskem či kopírováním zadat na tiskárně své jedinečné osobní číslo, alokovat každou tiskovou úlohu na konkrétní

[228] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 15.

[229] Stížnost č. 588/13 podaná k Evropskému soudu pro lidská práva dne 27. prosince 2012, Věc Eric Libert proti Francii.

pracovní projekt a případné (ve smyslu § 316 odst. 1 ZP dovolené) soukromé tiskové úlohy výslovně označit s tím, že tyto budou např. každý měsíc sečteny a zaměstnanci předepsány k úhradě dle předem určeného sazebníku. Rovněž může zaměstnavatel každému zaměstnanci předem určit maximální počet stran, které bude oprávněn bez dalšího vytisknout. Pokud bude tento počet stran překročen, bude zaměstnanec moci dále tisknout pouze po alokaci jednotlivých tiskových úloh na konkrétní projekty, respektive mu budou soukromé tiskové úlohy účtovány. Výše uvedená omezení lze aplikovat též např. pouze na barevný tisk, který je pro zaměstnavatele nákladnější.

Pro každého zaměstnance bude veden seznam uskutečněných tiskových úloh, přičemž údaje o tisku bude zaměstnavatel oprávněn zpracovávat v rozsahu název souboru, datum a čas tisku a počet vytištěných stran. V případě dovoleného soukromého tisku by zaměstnanci měli být povinni tento soubor přejmenovat jako „soukromý“, aby z názvu souboru zaměstnavatel nemohl poznat, o jaký dokument se jednalo a nedocházelo tak k neoprávněným zásahům do soukromí zaměstnance.

2.6.4 Mystery shopping

Mystery shopping je praxe, kdy zaměstnavatel kontroluje, jak zaměstnanec vystupuje vůči zákazníkům, a to tak, že osoba pověřená zaměstnavatelem (agent) při komunikaci se zaměstnancem vystupuje jako běžný zákazník. Zpravidla se využívají techniky jako *mystery calling* nebo *mystery mailing*, jejichž účelem je zjistit, jak zaměstnanci jménem zaměstnavatele komunikují se zákazníky prostřednictvím telefonu či e-mailu.[230] Pořízená nahrávka nebo komunikace je pak následně předána zaměstnavateli k vyhodnocení.

Bude-li *mystery shopping* prováděn pouze nahodile, nebude zaměstnavatel povinen splnit podmínky stanovené v § 316 odst. 2 ZP.[231] Pokud by měl být využíván pravidelně, domnívám se, že jako závažný důvod ve smyslu § 316 odst. 2 ZP by mohlo obstát zvyšování kvality poskytovaných služeb a s tím související kontrola práce

[230] KADLECOVÁ, Tereza. Monitoring zaměstnanců. *Praktická personalistika*. 2015, roč. 3, č. 11 – 12, s. 23. ISSN 2336-5072.

[231] NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 234. ISSN 1210-6410.

zaměstnanců. Vycházím analogicky ze stanoviska ÚOOÚ k pořizování nahrávek telefonátů zaměstnanců se zákazníky.[232] V každém případě však *mystery shopping* bude představovat zpracování osobních údajů.[233] Ve vnitřním předpise by zaměstnavatel měl předem informovat zaměstnance, že k takovým kontrolám může docházet, a jakým způsobem budou vykonávány.

[232] ÚOOÚ: Stanovisko č. 5/2013: Pořizování hlasových záznamů v rámci elektronické komunikace při poskytování služeb z pohledu zákona o ochraně osobních údajů. Říjen 2013, s. 2 – 3.

[233] NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 234. ISSN 1210-6410.

3. Související otázky

3.1 Hodnocení pracovní výkonnosti zaměstnance na základě monitoringu

Metody monitoringu popsané v předchozí kapitole mají často sloužit též k hodnocení pracovní výkonnosti zaměstnanců. Kromě toho jsou na pracovištích zaváděna další opatření sledující pracovní výkon zaměstnance, např. aplikace monitorující počet hodin odpracovaných na určitých projektech (v advokátních kancelářích proslulých jako „*billable hours*"), počet získaných zakázek, ekonomický přínos konkrétního zaměstnance pro zaměstnavatele, apod.

Jak ovšem upozorňuje Mezinárodní organizace práce v čl. 5.6 svého (právně nezávazného) Kodexu ochrany osobních údajů zaměstnanců, výkonnost zaměstnanců by neměla být hodnocena pouze na základě osobních údajů shromážděných pomocí elektronického monitoringu.[234] Totéž pravidlo zakotvuje ZOOÚ na základě Směrnice 95/46/ES v § 11 odst. 6, podle něhož nesmí správce nebo zpracovatel osobních údajů bez ověření vydat nebo učinit žádné rozhodnutí, jehož důsledkem je zásah do právních a právem chráněných zájmů subjektu údajů výlučně na základě automatizovaného zpracování osobních údajů, ledaže je tak učiněno ve prospěch subjektu údajů a na jeho žádost. GDPR tuto zásadu upravuje v čl. 22, podle něhož má subjekt údajů právo „*nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká*." Výjimky z tohoto pravidla, které jsou v tomtéž článku GDPR dále upraveny, nejsou dle mého názoru na pracovněprávní vztahy použitelné. V recitálu 71 GDPR se dále upřesňuje, že pomocí automatizovaného zpracování nemají být hodnoceny ani osobní aspekty daného subjektu údajů.

Není proto možné, aby zaměstnavatel vyvozoval pro zaměstnance pracovněprávní důsledky pouze na základě výsledků automatizovaného monitoringu, např. sledoval pomocí specifického softwaru počet hodin strávených na pracovních projektech, a se

[234] MEZINÁRODNÍ ORGANIZACE PRÁCE: *Kodex ochrany osobních údajů zaměstnanců* (v originále: „*Protection of Worker's Personal Data*"). 1. vydání. Ženeva: International Labour Office, 1997. ISBN 92-2-110329-3.

zaměstnancem, který by jich měl nejméně, bez dalšího rozvázal pracovní poměr.[235] Obdobně není možné, aby zaměstnavatel pouze na základě takového softwaru automaticky rozhodoval o výši bonusů, které mají zaměstnanci obdržet za daný měsíc nebo kalendářní rok.[236]

Výsledky monitoringu sice v praxi budou představovat podklad pro rozhodování zaměstnavatele, musejí však být podrobeny dalšímu zkoumání s přihlédnutím ke všem okolnostem týkajícím se daného zaměstnance. Ostatně hodnocení pracovní výkonnosti a pracovních výsledků podřízených zaměstnanců patří mezi základní povinnosti vedoucích zaměstnanců stanovené v § 302 písm. a) ZP.

3.2 Problematika BYOD

BYOD (z anglického „*Bring Your Own Device*“) je řešení, kdy zaměstnanci se souhlasem zaměstnavatele užívají vlastní zařízení, konkrétně mobilní telefon nebo počítač, k výkonu práce pro zaměstnavatele. Není neobvyklé, že tuto praxi žádají sami zaměstnanci, např. proto, že nechtějí používat a nosit při sobě dva mobilní telefony. Ostatně zaměstnavatel není oprávněn zaměstnancům BYOD jednostranně nařídit, a to s ohledem na jednu ze zásad závislé práce, podle níž musí být tato vykonávána na náklady zaměstnavatele. S ohledem na tento princip bude také zaměstnavatel povinen zaměstnancům za opotřebení jejich vlastního zařízení poskytovat odpovídající náhradu, a to některým z postupů uvedených v § 190 odst. 1 ZP.

Pro zaměstnavatele bude BYOD na jednu stranu představovat úsporu často nemalých nákladů na pořízení příslušných zařízení, na stranu druhou však přinese zvýšená rizika, co se možnosti zneužití dat zaměstnavatele týče. Zaměstnavatelé tak budou muset řešit, jak budou zařízení ve vlastnictví zaměstnanců zabezpečována proti virům, malwaru a dalším nežádoucím programům, kdo bude zajišťovat jejich servis, apod. Svá specifika

---

[235] Viz též KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel: *Zákon o ochraně osobních údajů. Komentář.* 1. vydání. Praha: C. H. Beck, 2012, s. 220. ISBN 978-80-7179-226-0.

[236] NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohumil, TOMÍŠEK, Jan. *GDPR / Obecné nařízení o ochraně osobních údajů*. 1. vydání. Praha: Wolters Kluwer Česká republika, 2017, dostupné elektronicky v systému ASPI. Komentář k čl. 22 GDPR, kapitola III. ISBN 978-80-7552-765-3.

bude mít pochopitelně také situace, kdy se zaměstnavatel rozhodne tato zařízení podrobit určité formě monitoringu. Ten totiž nesmí zasahovat do ryze soukromých sekcí daného zařízení (např. fotografie) a, jak upozorňuje Pracovní skupina, přijatá sledovací opatření musejí být schopna striktně rozlišovat užívání daného zařízení pro soukromé a pro pracovní účely. V ideálním případě by proto měla být veškerá pracovní data soustředěna do jedné či více zcela oddělených aplikací, jejichž užívání pak může být předmětem monitoringu.[237]

Přeje-li si zaměstnavatel umožnit zaměstnancům BYOD řešení (respektive je z důvodů úspory vlastních nákladů k akceptaci tohoto řešení motivovat), měl by vydat vnitropodnikovou směrnici, v níž budou popsána práva a povinnosti zaměstnanců i zaměstnavatele s ohledem na užívání daného zařízení, včetně způsobu a podmínek jeho případného monitoringu. Pokud se zaměstnanci rozhodnou BYOD využít, měli by tyto podmínky výslovně akceptovat, a to nejlépe smluvně.

3.3 Postih zaměstnanců na základě skutečností zjištěných prostřednictvím monitoringu

Z výsledků prováděného monitoringu mohou vyjít najevo skutečnosti, na jejichž základě bude zaměstnavatel oprávněn proti danému zaměstnanci přijmout určitá pracovněprávní opatření. Konkrétní podoba takového opatření bude záviset na intenzitě a míře závažnosti porušení povinnosti zaměstnance vyplývající z právních předpisů vztahujících se k jím vykonávané práci. Nejmírnějším z nich může být nepřiznání či snížení výše bonusu, pokud je podmínkou jeho výplaty kromě jiných okolností též dodržování povinností zaměstnance a řádný výkon práce, jak tomu zpravidla bývá. Další opatření pak většinou směřují k rozvázání pracovního poměru výpovědí podle § 52 písm. g) ZP, a to (i) rovnou, pokud půjde o závažné porušení povinností zaměstnance nebo o důvod, pro který by bylo možné pracovní poměr zrušit okamžitě, nebo (ii) s předchozím upozorněním na možnost výpovědi, pokud půjde o soustavné méně závažné porušování povinností. V případě porušení povinností zaměstnance

[237] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017, s. 17.

zvlášť hrubým způsobem pak může zaměstnavatel přistoupit k okamžitému zrušení pracovního poměru dle § 55 odst. 1 písm. b) ZP. Okamžité zrušení pracovního poměru na základě monitoringu autorizoval Nejvyšší soud a posléze též Ústavní soud v případě popsaném v kapitole 1.5.2(b) výše.

V souvislosti s vyvozováním jakýchkoli důsledků ze zjištěných případů porušování pracovních povinností zaměstnance však musí zaměstnavatel pamatovat na zásadu rovného zacházení. Není možné, aby zaměstnavatel sankcionoval jen jednoho konkrétního zaměstnance (např. proto, že je s ním dlouhodobě nespokojen, avšak obtížně hledá zákonný důvod k jeho propuštění), přestože výsledky monitoringu odhalily porušování povinností též ze strany jiných zaměstnanců. Rovněž není přípustná praxe, kdy zaměstnavatel ví a dlouhodobě fakticky toleruje užívání pracovních prostředků ze strany zaměstnanců k soukromým účelům, aniž jim to výslovně dovolil, ovšem následně za toto jednání postihne jen některého ze zaměstnanců, ať už stávajících, či nově nastupujících. Kromě toho, ustanovení § 316 odst. 1 ZP pro souhlas zaměstnavatele nepředepisuje žádnou formu, tudíž tento může být dán i konkludentně.[238]

V případě soudního sporu se zaměstnancem o neplatnost výpovědi nebo o náhradu škody způsobené zaměstnancem se zaměstnavatel jistě bude chtít bránit důkazními prostředky pořízenými v rámci monitoringu. Pokud zaměstnavatel zavedl monitoring v souladu s § 316 odst. 2 a 3 ZP, po splnění testu proporcionality a případně též v souladu s relevantními ustanoveními ZOOÚ (respektive GDPR), bude takový důkaz jistě přípustný.

České soudy se nicméně mnohokrát zabývaly situací, kdy strana sporu navrhla provedení důkazu, jenž nebyl pořízen plně v souladu s právními předpisy; často přitom nicméně došly ke zcela opačným závěrům. Jedním z nich je již výše zmiňovaný rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1009/98 ze dne 21. října 1998 (viz kapitolu 2.5.4(b) výše), v němž soud dospěl k závěru, že důkaz záznamem telefonických hovorů zaměstnanců, jenž byl pořízen bez jejich vědomí, není přípustný.[239]

---

[238] MORÁVEK, Jakub. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy.* 2017, roč. 25, č. 17, s. 576. ISSN 1210-6410.

[239] Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1009/98 ze dne 21. října 1998.

Takřka opačný závěr pak přinesl rozsudek Nejvyššího soudu sp. zn. 30 Cdo 64/2004 ze dne 11. května 2005, v němž soud konstatoval, že zvukový záznam zachycující projevy, ke kterým dochází při výkonu povolání, při obchodní či veřejné činnosti, zpravidla nelze považovat za zaznamenání projevu osobní povahy, a důkaz takovým záznamem v občanském soudním řízení proto připustil.[240] Tento názor byl ovšem v dalším pracovněprávním rozsudku Nejvyššího soudu sp. zn. 21 Cdo 434/2010 ze dne 9. března 2011 označen za vybočení z ustálené judikatury soudů a soud se přiklonil k dříve zastávanému stanovisku ohledně nepřípustnosti důkazu v podobě nahrávky pořízené bez souhlasu příslušných osob. Zde ovšem byla situace taková, že nahrávku rozhovoru pořídil zaměstnanec, aby prokázal, že organizační změna, v jejímž důsledku dostal výpověď, byla pouze účelová. Ve skutečnosti se jej zaměstnavatel chtěl zbavit, protože jej zaměstnanec kritizoval u zahraničního vedení zaměstnavatele, což bylo patrné právě z rozhovoru zachyceného na nahrávce.[241] Případ se ovšem dostal až k Ústavnímu soudu, který se zastal zaměstnance a poukázal opět na názor vyslovený v rozsudku Nejvyššího soudu sp. zn. 30 Cdo 64/2004. Rovněž konstatoval, že za běžných okolností je svévolné nahrávání soukromých rozhovorů bez vědomí jejich účastníků hrubým zásahem do jejich soukromí. Pokud však tajné pořízení audiozáznamu rozhovoru (obsahuje-li vůbec projevy osobní povahy) představuje způsob dosažení právní ochrany pro výrazně slabší stranu významného občanskoprávního a zejména pracovněprávního sporu, je zásah do práva na soukromí osoby, jejíž mluvený projev je zaznamenán, plně ospravedlnitelný zájmem na ochraně slabší strany právního vztahu, jíž hrozí závažná újma (včetně např. ztráty zaměstnání). Opatření jediného nebo klíčového důkazu touto cestou je dle Ústavního soudu analogické k jednání za podmínek krajní nouze či dovolené svépomoci.[242]

Je však otázkou, zda a v jakých situacích by výše uvedený závěr Ústavního soudu mohl použít též zaměstnavatel jako zpravidla podstatně silnější smluvní strana pracovněprávního vztahu. Pravděpodobně to vzhledem k principu proporcionality bude možné tehdy, pokud by újma hrozící zaměstnavateli byla nepoměrně vyšší než újma

[240] Rozsudek Nejvyššího soudu sp. zn. 30 Cdo 64/2004 ze dne 11. května 2005.

[241] Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 434/2010 ze dne 9. března 2011.

[242] Nález Ústavního soudu sp. zn. II. ÚS 1774/14 ze dne 9. prosince 2014.

hrozící zaměstnanci v důsledku porušení jeho práva na ochranu soukromí. S ohledem na dostupnou judikaturu to budou zásadně situace, kdy se bude jednat o trestný čin.[243]

Nezajímavý v tomto kontextu není ani názor Nejvyššího správního soudu k možnosti použití důkazu z kamerového systému, který nebyl řádně registrován u ÚOOÚ. Soud došel k závěru, že zápis do registru vedeného ÚOOÚ má pouze ty účinky, že „*aprobuje, že bude-li oznámený kamerový systém provozován v souladu s podmínkami oznámení (§ 16 odst. 2 zákona), dochází jím ke zpracování osobních údajů v souladu se zákonem. Provozování kamerového systému bez tohoto oznámení má tak (kromě sankční odpovědnosti provozovatele – srov. § 44 odst. 2 písm. i) a § 45 odst. 1 písm. i) zákona) pouze ten následek, že má-li být jím pořízený záznam použit jako důkaz ve správním či soudním řízení, bude nutné provést celkové posouzení, zda docházelo ke zpracovávání osobních údajů v rozporu se zákonem či nikoliv. Pro opačný závěr, tedy že provozování kamerového systému bez předchozího oznámení a zápisu do registru má bez dalšího za následek neoprávněnost zpracovávání osobních údajů, nelze v zákoně nalézt oporu*.“[244] Nejvyšší správní soud rovněž vzpomenul názor Ústavního soudu, že ačkoli je nesplnění oznamovací povinnosti vůči ÚOOÚ přestupkem, „*nelze jej hodnotit jako porušení právního předpisu takové závažnosti, která by měla za následek absolutní neúčinnost důkazu získaného průmyslovou kamerou. Jedná se o formální pochybení v záležitosti administrativního charakteru ve vztahu ke správnímu orgánu, které však nutně neimplikuje neoprávněnost instalace záznamového zařízení či nepřípustnost důkazního prostředku takto pořízeného*.“[245]

---

[243] Viz např. rozsudek Nejvyššího soudu sp. zn. 5 Tdo 459/2007 ze dne 3. května 2007: „*S ohledem na ustanovení § 89 odst. 2 tr. ř. zásadně nelze vyloučit možnost, aby byl k důkazu použit i zvukový záznam, který byl pořízen soukromou osobou bez souhlasu osob, jejichž hlas je takto zaznamenán. Ustanovení § 88 tr. ř. se zde neuplatní, a to ani analogicky. Přípustnost takového důkazu je však nezbytné vždy posuzovat též s ohledem na respektování práva na soukromí zakotveného v čl. 8 Úmluvy o ochraně lidských práv a základních svobod a práva na nedotknutelnost osoby a jejího soukromí ve smyslu čl. 7 odst. 1 a čl. 10 odst. 2 Listiny základních práv a svobod*.“

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

[245] Usnesení Ústavního soudu sp. zn. IV. ÚS 2425/09 ze dne 8. února 2010.

3.4 Prostředky obrany zaměstnance proti monitoringu

Domnívá-li se zaměstnanec, že jej zaměstnavatel monitoruje v rozporu se ZP, může předně podat podnět k příslušnému orgánu inspekce práce k provedení kontroly u zaměstnavatele. Jak již bylo uvedeno v kapitole 1.5.2(g) výše, jsou orgány inspekce práce nově s účinností od 29. července 2017 oprávněny zavedení monitoringu v rozporu s § 316 odst. 2 ZP a nesplnění informační povinnosti dle § 316 odst. 3 ZP pokutovat jako přestupek. Než došlo k tomuto rozšíření sankčních kompetencí orgánů inspekce práce, byly případy domněle nezákonného monitoringu postupovány ÚOOÚ, aby jednání zaměstnavatele mohlo být alespoň nějakým veřejnoprávním způsobem postižitelné. Pokud však daný monitoring zároveň nepředstavoval zpracování osobních údajů (jako např. kamerový systém v online režimu bez záznamu), nebyl ÚOOÚ oprávněn zasáhnout, a zaměstnanec tak mohl neoprávněnost monitoringu napadnout pouze prostřednictvím žaloby na ochranu osobnosti v občanskoprávním řízení.

I po výše uvedených změnách je zaměstnanec oprávněn podat podnět k provedení kontroly u zaměstnavatele též k ÚOOÚ, a to v případě, kdy se bude domnívat, že zaměstnavatel monitoringem porušuje ZOOÚ (např. zpracovává více údajů, než je pro daný účel nezbytné, shromážděné údaje uchovává po delší než přiměřenou dobu nebo porušuje jiné zásady zpracování osobních údajů). Nově se má tedy ÚOOÚ zaměřit pouze na vlastní oblast působnosti, a to na případy porušování ochrany osobních údajů garantované ZOOÚ. Dle důvodové zprávy k zákonu č. 206/2017 Sb., který zavedl výše uvedenou pravomoc orgánů inspekce práce pokutovat neoprávněný monitoring, mají nicméně ÚOOÚ a orgány inspekce práce v oblasti ochrany soukromí zaměstnance vzájemně spolupracovat, zejména si předávat podněty ke kontrole dle oblasti svých kompetencí.[246]

V soukromoprávní oblasti se zaměstnanec může domáhat svých práv prostřednictvím žaloby na ochranu osobnosti. V souladu s § 82 OZ může zaměstnanec žádat, aby bylo od neoprávněného zásahu (monitoringu) upuštěno a aby byl odstraněn jeho následek, pokud stále trvá. Zároveň může požadovat náhradu újmy, která mu byla na jeho přirozeném právu (na ochranu soukromí) v důsledku zásahu způsobena, přičemž dle

[246] Vládní návrh zákona, kterým se mění zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a další související zákony. Sněmovní tisk č. 911/0, s. 53.

§ 2956 OZ bude oprávněn požadovat náhradu škody i nemajetkové újmy. Jako nemajetková újma mají být odčiněny též způsobené duševní útrapy. Dle § 2951 odst. 1 OZ se škoda nahrazuje uvedením do předešlého stavu; není-li to dobře možné, anebo žádá-li to poškozený, hradí se škoda v penězích. Neoprávněným monitoringem však zaměstnanci bude způsobena spíše než majetková škoda nemajetková újma. Ta se má dle § 2951 odst. 2 OZ odčinit přiměřeným zadostiučiněním s tím, že toto musí být poskytnuto v penězích, nezajistí-li jeho jiný způsob skutečné a dostatečně účinné odčinění způsobené újmy.

V praxi se však zaměstnanci ochrany své osobnosti v rámci občanskoprávního řízení zpravidla nedomáhají, a relevantní rozhodovací praxe proto chybí.[247] Přitom i tehdy, kdy orgán inspekce práce/ÚOOÚ konstatuje porušení právních předpisů ze strany zaměstnavatele, musí se zaměstnanec případné náhrady nemajetkové újmy (a též případné škody, nebyla-li její výše spolehlivě zjištěna) domáhat právě v občanskoprávním řízení, kam jej správní orgán s jeho nárokem odkáže. Nepominutelným faktorem odrazujícím zaměstnance od podání žaloby však jistě budou náklady řízení, zdlouhavost soudního řízení a jeho nejistý výsledek.

Zaměstnanec si samozřejmě může na zavedené prostředky monitoringu stěžovat také přímo u zaměstnavatele. V souladu s § 276 odst. 9 ZP je zaměstnavatel povinen projednat se zaměstnancem (nebo na jeho žádost s odborovou organizací nebo radou zaměstnanců) stížnost zaměstnance na výkon práv a povinností vyplývajících z pracovněprávních vztahů. Tento postup je ryze dobrovolný; obvykle však zřejmě ke změně názoru zaměstnavatele na sledování zaměstnance nepovede.

[247] ZEMANOVÁ ŠIMONOVÁ, Hana. Právní prostředky ochrany osobnosti zaměstnance. *Bulletin advokacie*. 2016, č. 10, s. 44. ISSN 1210-6348.

Závěr

Záměrem této práce bylo poskytnout co nejvyváženější právní pohled na problematiku sledování zaměstnanců, a to jak z hlediska práv a oprávněných zájmů zaměstnavatele, tak z hlediska práva zaměstnanců na soukromí. S technologickým rozvojem přitom otázka monitoringu zaměstnanců postupně nabývá na aktuálnosti; čím dál více zaměstnanců totiž k výkonu své práce využívá internet, mobilní telefony a počítače, které jim zaměstnavatelé za tímto účelem svěřují. Ti si však pochopitelně přejí mít určitý přehled ohledně užívání těchto zařízení, zejména s cílem bránit jejich případnému zneužívání, a to ať už k soukromým účelům (pokud to není dovoleno), nebo za účelem (nedbalostního či dokonce úmyslného) poškozování zaměstnavatele. Technologický pokrok rovněž přináší nové, sofistikovanější a dostupnější možnosti co se sledování zaměstnanců týče. Ty ovšem mohou vést k podstatným zásahům do soukromí zaměstnanců a k vyšší míře rizika zneužitelnosti jejich osobních údajů, které jsou ve většině případů monitoringu shromažďovány a jinak zpracovávány. Proto je v rámci každého monitoringu nezbytné vždy nalézt vzájemnou rovnováhu mezi právy a zájmy zaměstnavatele a právem sledovaných zaměstnanců na soukromí.

Jak z této práce a z uváděných případů z rozhodovací praxe vyplývá, nejdůležitějším klíčem k hledání této rovnováhy je princip proporcionality. Není to vždy jednoznačný princip a do určité míry podléhá a nadále bude podléhat tendenčním změnám jeho výkladu; otázkou do budoucna je, zda tyto změny povedou ve prospěch práv zaměstnavatelů nebo naopak zaměstnanců. Vyhodnocování testu proporcionality, k němuž musí před upřednostněním jednoho práva před druhým vždy dojít, není v praxi vždy jednoduché. Cílem této práce proto bylo nabídnout určitá vodítka, jak rovnováhy práv obou stran dosáhnout, a to kromě jiného na příkladu konkrétních návrhů scénářů monitoringu pro každé z nejčastěji používaných sledovacích opatření.

V této práci rozlišuji (i) tzv. jednorázovou či nahodilou kontrolu zaměstnanců prováděnou za účelem ověření dodržování zákazu užívání výrobních a pracovních prostředků zaměstnavatele pro jejich osobní potřebu ve smyslu § 316 odst. 1 ZP a (ii) soustavný monitoring zaměstnanců (tzv. monitoring v užším slova smyslu) dle § 316 odst. 2 ZP. Následně je třeba rozlišovat, zda při monitoringu dochází ke zpracování osobních údajů zaměstnanců či nikoli. Pokud všechna tato kritéria sečteme,

zjistíme, že je třeba pracovat s celkem čtyřmi typy kontrol/sledování zaměstnanců. Každý z nich má přitom relativně odlišný právní režim.

Shodně s částí literatury (viz kapitolu 1.4, str. 20) docházím k závěru, že pro jednorázovou či nahodilou kontrolu nemusí zaměstnavatel splnit podmínku závažného důvodu spočívajícího ve zvláštní povaze své činnosti (tato kontrola musí však být dle § 316 odst. 1 ZP provedena přiměřeným způsobem). S ohledem na jazykový výklad ustanovení § 316 odst. 2 ZP konstatuji, že zde uvedenou podmínku je třeba splnit pouze v případě zvláště intenzivního, systematického a dlouhodobého sledování zaměstnanců. Ostatně pokud by kontrolu dodržování zákazu dle § 316 odst. 1 ZP nemohl provést každý zaměstnavatel, který svým zaměstnancům svěří vlastní pracovní prostředky, bylo by to dle mého názoru v rozporu s jeho ústavně zaručeným právem na ochranu majetku.

Právní úprava týkající se kontrol a sledování zaměstnanců dle ustanovení § 316 ZP je sice v nenovelizované podobě účinná již od 1. ledna 2007, přesto však není rozhodovací praxe na toto téma příliš rozsáhlá. Dokonce ani výklad základní podmínky soustavného monitoringu dle § 316 odst. 2 ZP, tj. pojmu závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele, bez něhož nelze tento typ monitoringu zavést, nebyl ze strany českých soudů zcela jednoznačně podán. Pokud bychom se navíc zabývali pouze rozhodnutími obou nejvyšších soudů, potažmo Ústavního soudu, pak vlastně tento pojem nebyl dosud komplexně vyložen vůbec. Relativně restriktivní výklad pojmu zvláštní činnosti ovšem zastává ÚOOÚ, který ji zásadně přiznává pouze zaměstnavatelům vykonávajícím skutečně nebezpečnou či nějakým způsobem jinak výjimečnou podnikatelskou činnost (např. provádění mezinárodních bankovních převodů a jiné nakládání s vysokými finančními částkami, dozor nad prací vězňů, manipulace s vysoce nebezpečnými chemikáliemi apod.; blíže viz kapitolu 1.4, str. 17). V této práci se však ztotožňuji s názorem, který v odborné literatuře převažuje a podle něhož lze právo monitorovat vlastní zaměstnance při splnění určitých podmínek (zejména testu proporcionality) přiznat v podstatě každému zaměstnavateli. Nejednoznačný přístup k výkladu pojmu závažného důvodu spočívajícího ve zvláštní povaze činnosti však zaměstnavatelům a jejich právním poradcům v praxi značně komplikuje situaci, neboť přináší právní nejistotu ohledně legitimity zaváděných sledovacích opatření.

Pokud jednorázová kontrola či soustavný monitoring zaměstnanců představuje též zpracování jejich osobních údajů, jsou zaměstnavatelé zároveň povinni plnit řadu podmínek vyplývajících z právní úpravy na ochranu osobních údajů. Ta v současné době prochází zřejmě nejvýznamnější změnou za posledních více než 20 let. S účinností od 25. května 2018 totiž bude stávající Směrnice 95/46/ES nahrazena novým GDPR jako přímo použitelným právním předpisem, a to s ambiciózním (i když zřejmě ne úplně realistickým) cílem sjednotit právní úpravu ochrany osobních údajů ve všech členských státech Evropské unie. Co se týče české právní úpravy, bude ZOOÚ zřejmě zrušen a nahrazen zcela novým právním předpisem, který bude nadále upravovat pouze postavení ÚOOÚ a otázky, jež GDPR svěřuje členským státům k národní právní úpravě.

Pro zaměstnavatele jako správce osobních údajů bude GDPR znamenat řadu nových povinností, jež samozřejmě budou mít nemalý vliv i na monitoring zaměstnanců. Tato práce se snaží tyto povinnosti přiblížit, a to na základě dosud dostupných zdrojů, zejména relevantních výkladových stanovisek vydaných Pracovní skupinou. Lze konstatovat, že v řadě ohledů bude po účinnosti GDPR obtížnější a nákladnější monitoring se zpracováním osobních údajů zavést, a to zejména vzhledem k přísnějším požadavkům na zabezpečení osobních údajů. Menším zaměstnavatelům se tak ani nemusí monitoring s přihlédnutím k jeho administrativní a finanční náročnosti vyplatit.

Novinkou je též oprávnění orgánů inspekce práce pokutovat zaměstnavatele za (i) narušování soukromí zaměstnanců některým ze způsobů uvedených v § 316 odst. 2 ZP a (ii) neplnění informační povinnosti v souvislosti s monitoringem dle § 316 odst. 3 ZP. Tuto novou kompetenci jim zákonodárce svěřil s účinností od 29. července 2017 poté, co byl její nedostatek již řadu let předtím terčem kritiky zejména ze strany Veřejného ochránce práv. Nyní je otázkou, jak orgány inspekce práce se svým novým oprávněním naloží a jakým způsobem se to promítne do praxe v zavádění sledovacích opatření. Bude-li inspekce práce monitoring zaměstnanců kontrolovat důsledně, pravděpodobně se v této oblasti dočkáme bohatší rozhodovací praxe též českých soudů. Po více než deseti letech od účinnosti ZP tak možná již brzy bude podán komplexní výklad pojmu závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele dle § 316 odst. 2 ZP a v oblasti monitoringu zaměstnanců nastolena větší právní jistota.

Seznam použitých zdrojů

Dokumenty

1. EDPS: Zásady video monitoringu vydané EDPS (v originále: „*The EDPS Video-Surveillance Guidelines*“). Brusel, 17. března 2010.

2. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 8/2001 o zpracování osobních údajů v kontextu zaměstnání (v originále: „*Opinion 8/2001 on the processing of personal data in the employment context*“) ze dne 13. září 2001.

3. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Pracovní dokument o sledování elektronických komunikací na pracovišti (v originále: „*Working document on the surveillance of electronic communications in the workplace*“) ze dne 29. května 2002.

4. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 4/2004 o zpracování osobních údajů pomocí kamerových systémů (v originále: „*Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*“) ze dne 11. února 2004.

5. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko ohledně užívání lokačních údajů s přihlédnutím k poskytování služeb s přidanou hodnotou (v originále: „*Opinion on the use of location data with a view to providing value-added services*“) ze dne 25. listopadu 2005.

6. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 4/2007 k pojmu osobních údajů (v originále: „*Opinion 4/2007 on the concept of personal data*“) ze dne 20. června 2007.

7. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 13/2011 o geolokalizačních službách u inteligentních mobilních zařízení (v originále: „*Opinion 13/2011 on Geolocation services on smart mobile devices*“) ze dne 16. května 2011.

8. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 15/2011 o definici souhlasu (v originále: „*Opinion 15/2011 on the definition of consent*“) ze dne 13. července 2011.

9. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 3/2012 o pokrocích v oblasti biometrických technologií (v originále: „*Opinion 3/2012 on developments in biometric technologies*“) ze dne 27. dubna 2012.

10. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 03/2013 o omezení účelem (v originále: „*Opinion 03/2013 on purpose limitation*“) ze dne 2. dubna 2013.

11. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Výkladové stanovisko k pověřencům pro ochranu osobních údajů (v originále: „*Guidelines on Data Protection Officers (DPOs)*“) ze dne 13. prosince 2016.

12. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Příloha k Výkladovému stanovisku k pověřencům pro ochranu osobních údajů (v originále: „*Guidelines on Data Protection Officers (DPOs)*“) ze dne 13. prosince 2016 – Často kladené otázky (v originále „*Frequently Asked Questions*“).

13. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Výkladové stanovisko k posouzení vlivu na ochranu osobních údajů a určení, zda je pravděpodobné, že zpracování bude mít za následek vysoké riziko, pro účely Nařízení 2016/679 (v originále: „*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679*“) ze dne 4. dubna 2017.

14. Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 2/2017 o zpracování osobních údajů v práci (v originále: „*Opinion 2/2017 on data processing at work*“) ze dne 8. června 2017.

15. Státní úřad inspekce práce, odbor pracovních vztahů a podmínek: Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele. Srpen 2010.

16. Státní úřad inspekce práce, odbor pracovních vztahů a podmínek: Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele. Leden 2011.

17. Státní úřad inspekce práce, odbor pracovních vztahů a podmínek: Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele. Květen 2014.

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

19. ÚOOÚ: Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Leden 2006.

20. ÚOOÚ: Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2007.

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

22. ÚOOÚ: Stanovisko č. 3/2009: Biometrická identifikace nebo autentizace zaměstnanců. Květen 2009.

23. ÚOOÚ: Informační bulletin 2/2011. Prosinec 2011.

24. ÚOOÚ: Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2010. Brno: Masarykova univerzita, 2011, 73 s. ISBN 978-80-210-5428-8.

25. ÚOOÚ: Stanovisko č. 5/2013: Pořizování hlasových záznamů v rámci elektronické komunikace při poskytování služeb z pohledu zákona o ochraně osobních údajů. Říjen 2013.

26. ÚOOÚ: Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2013. Brno: Nakladatelství MU Brno, 2014, 85 s. ISBN 978-80-210-6700-4.

27. ÚOOÚ: Provozování kamerových systémů. Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů. Brno: Masarykova univerzita, 2012, 29 s. ISBN 978-80-210-6017-3.

28. ÚOOÚ: Ochrana osobních údajů na pracovišti. Příručka pro zaměstnance. Brno: Masarykova univerzita, 2014, 36 s. ISBN 978-80-210-6819-3.

29. ÚOOÚ: Věstník Úřadu pro ochranu osobních údajů. Částka 73, srpen 2017, s. 4131.

30. Vládní návrh zákona, kterým se mění zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a další související zákony. Sněmovní tisk č. 911/0.

31. Výbor ministrů Rady Evropy: Doporučení Výboru ministrů členským státům č. CM/Rec(2015)5 ohledně zpracování osobních údajů v kontextu zaměstnání.

Neperiodická literatura

1. BĚLINA, Miroslav a kolektiv. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015, xviii, 1610 s. Velké komentáře. ISBN 978-80-7400-290-8.

2. BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi*. 2. vyd. Praha: LINDE, 2010, 264 s. ISBN 978-80-7201-817-8.

3. BARTÍK, V., JANEČKOVÁ, E. *Kamerové systémy v praxi*. 1. vyd. Praha: LINDE, 2011, dostupné elektronicky v systému ASPI. ISBN 978-80-7201-850-5.

4. KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel: *Zákon o ochraně osobních údajů. Komentář.* 1. vydání. Praha: C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0.

5. MEZINÁRODNÍ ORGANIZACE PRÁCE: *Kodex ochrany osobních údajů zaměstnanců* (v originále: „*Protection of Worker's Personal Data*"). 1. vydání. Ženeva: International Labour Office, 1997, 24 s. ISBN 92-2-110329-3.

6. MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. 1. vydání. Praha: Wolters Kluwer ČR, 2013, dostupné elektronicky v systému ASPI. ISBN 978-80-7478-139-1.

7. NULÍČEK, Michal, DONÁT, Josef, NONNEMANN, František, LICHNOVSKÝ, Bohumil, TOMÍŠEK, Jan. *GDPR / Obecné nařízení o ochraně osobních údajů*.

1. vydání. Praha: Wolters Kluwer Česká republika, 2017, dostupné elektronicky v systému ASPI. ISBN 978-80-7552-765-3.

Periodická literatura

1. BARTÍK, Václav, JANEČKOVÁ, Eva. Kamery se záznamovým zařízením na pracovišti. *Práce a mzda*. 2010, č. 3. ISSN 0032-6208. Dostupné z WWW: <http://www.mzdovapraxe.cz/archiv/dokument/doc-d9135v11954-kamery-se-zaznamovym-zarizenim-na-pracovisti/?search_query=%24issue%3D3I97&order_by=&order_dir=&type=&search_results_page=1>.

2. DURUGY, Andras, KOLLAR, Peter. On the Use of Mystery Shopping to Measure Competences. *Journal of Human Resource Management*. 2017, roč. XX, č. 1, s. 81 – 88. ISSN 2453-7683.

3. JOUZA, Ladislav. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. *Bulletin advokacie*. 2014, č. 6, s. 26 – 30. ISSN 1210-6348.

4. KADLECOVÁ, Tereza. Monitoring zaměstnanců. *Praktická personalistika*. 2015, roč. 3, č. 11 – 12, s. 22 – 28. ISSN 2336-5072.

5. LACHAUD, Erich. Why the certification process defined in the General Data Protection Regulation cannot be successful. *Computer Law & Security Review*. 2016, roč. 32, č. 6, s. 814-826. ISSN 0267-3649.

6. MORÁVEK, Jakub. Osobní potřeba – neurčitý právní pojem? *Právní rozhledy*. 2010, roč. 18, č. 24, s. 867 – 872. ISSN 1210-6410.

7. MORÁVEK, Jakub. Kdy lze jako důkazní prostředek připustit záznam z kamerového systému? *Právní rozhledy*. 2011, roč. 19, č. 13, s. 457 – 463. ISSN 1210-6410.

8. MORÁVEK, Jakub. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy*. 2017, roč. 25, č. 17, s. 573 – 581. ISSN 1210-6410.

9. NONNEMANN, František. Soukromí na pracovišti. *Právní rozhledy*. 2015, roč. 23, č. 7, s. 229 – 236. ISSN 1210-6410.

10. RADIČOVÁ, Zuzana. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy*. 2014, roč. 22, č. 21, s. 736 – 740. ISSN 1210-6410.

11. ZEMANOVÁ ŠIMONOVÁ, Hana. Právní prostředky ochrany osobnosti zaměstnance. *Bulletin advokacie*. 2016, č. 10, s. 40 – 44. ISSN 1210-6348.

Právní předpisy

1. Mezinárodní pakt o občanských a politických právech, vyhlášen ve Sbírce zákonů pod č. 120/1976 Sb.

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. 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.

4. Smlouva o Evropské unii, konsolidované znění. Úřední věstník Evropské unie, 2012/C 326/1, 26. října 2012.

5. Smlouva o fungování Evropské unie, konsolidované znění. Úřední věstník Evropské unie, 2012/C 326/1, 26. října 2012.

6. Úmluva o ochraně lidských práv a základních svobod ve znění protokolů č. 3, 5 a 8, vyhlášená ve Sbírce zákonů pod č. 209/1992 Sb.

7. Úmluva č. 108 Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat z roku 1981, vyhlášená ve Sbírce mezinárodních smluv České republiky pod č. 115/2001 Sb. m. s.

8. Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů.

9. Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.
10. Všeobecná deklarace lidských práv.
11. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
12. Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.
13. Zákon č. 251/2005 Sb., o inspekci práce, ve znění pozdějších předpisů.
14. Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.
15. Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.
16. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
17. Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.
18. Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
19. Zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů.
20. Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich.

Rozhodovací praxe

1. Nález Ústavního soudu sp. zn. Pl. ÚS 4/94 ze dne 12. října 1994.
2. Nález Ústavního soudu sp. zn. I. ÚS 321/06 ze dne 18. prosince 2006.
3. Nález Ústavního soudu sp. zn. Pl. ÚS 52/13 ze dne 9. září 2014.
4. Nález Ústavního soudu sp. zn. II. ÚS 1774/14 ze dne 9. prosince 2014.
5. Rozhodnutí předsedy Úřadu pro ochranu osobních údajů, č. j. UOOU-00363/13-41 ze dne 24. dubna 2013.
6. Rozhodnutí Úřadu pro ochranu osobních údajů, č. j. UOOU-00237/13-38 ze dne 3. července 2013.

7. Rozsudek Evropského soudu pro lidská práva, stížnost č. 13710/88, ze dne 16. prosince 1992, Věc Niemietz proti Německu.
8. Rozsudek Evropského soudu pro lidská práva, stížnost č. 20605/92, ze dne 25. června 1997, Věc Halfordová proti Spojenému království.
9. Rozsudek Evropského soudu pro lidská práva, stížnost č. 62617/00, ze dne 3. dubna 2007, Věc Coplandová proti Spojenému království.
10. Rozsudek Evropského soudu pro lidská práva, stížnost č. 420/07, ze dne 5. října 2010, Věc Karin Köpke proti Německu.
11. Rozsudek Evropského soudu pro lidská práva, stížnost č. 61496/08, ze dne 12. ledna 2016, Věc Bărbulescu proti Rumunsku.
12. Rozsudek Městského soudu v Praze sp. zn. 8A 182/2010 ze dne 2. září 2014.
13. Rozsudek Městského soudu v Praze sp. zn. 5 A 107/2013 ze dne 18. října 2016.
14. Rozsudek Městského soudu v Praze sp. zn. 6 A 42/2013 ze dne 5. května 2017.
15. Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1009/98 ze dne 21. října 1998.
16. Rozsudek Nejvyššího soudu sp. zn. 30 Cdo 64/2004 ze dne 11. května 2005.
17. Rozsudek Nejvyššího soudu sp. zn. 5 Tdo 459/2007 ze dne 3. května 2007.
18. Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 434/2010 ze dne 9. března 2011.
19. Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1771/2011 ze dne 16. srpna 2012.
20. Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 747/2013 ze dne 7. srpna 2014.
21. Rozsudek Nejvyššího správního soudu sp. zn. 3 As 21/2005 ze dne 10. května 2006.
22. Rozsudek Nejvyššího správního soudu sp. zn. 2 As 45/2010 ze dne 18. listopadu 2011.
23. Rozsudek Nejvyššího správního soudu sp. zn. 5 As 158/2012 ze dne 23. srpna 2013.

24. Rozsudek Soudního dvora (velkého senátu) ze dne 13. května 2014 ve věci C-131/12, Google Spain SL a Google Inc. v. Agencia Espanola de Protección de Datos (AEPD) a Mario Costeja González.

25. Stížnost č. 588/13 podaná k Evropskému soudu pro lidská práva dne 27. prosince 2012, Věc Eric Libert proti Francii.

26. Stížnost č. 70838/13 podaná k Evropskému soudu pro lidská práva dne 25. října 2013, Věc Nevenka Antović a Jovan Mirković proti Černé Hoře.

27. Usnesení Ústavního soudu sp. zn. I. ÚS 452/09 ze dne 31. března 2009.

28. Usnesení Ústavního soudu sp. zn. IV. ÚS 2425/09 ze dne 8. února 2010.

29. Usnesení Ústavního soudu sp. zn. I. ÚS 3933/12 ze dne 7. listopadu 2012.

Internetové zdroje

1. NONNEMANN, František. Sledování aktivity zaměstnance na internetu ve světle aktuální judikatury Evropského soudu pro lidská práva [online]. Publikováno dne 2. února 2016 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.epravo.cz/top/clanky/sledovani-aktivity-zamestnance-na-internetu-ve-svetle-aktualni-judikatury-evropskeho-soudu-pro-lidska-prava-100316.html>.

2. SLONKOVÁ, Sabina, JUNEK, Adam. Tajná schůzka před volbou prezidenta: Exkluzivní záznam [online]. Publikováno dne 4. února 2008 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://zpravy.aktualne.cz/domaci/tajna-schuzka-pred-volbou-prezidenta-exkluzivni-zaznam/r~i:article:520359/?redirected=1508444541>.

3. TaylorWessing LLP: Lawful processing of HR data under the GDPR [online]. Publikováno v březnu 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://united-kingdom.taylorwessing.com/globaldatahub/article-processing-of-hr-data-under-the-gdpr.html>.

4. ÚOOÚ: K problémům z praxe, č. 1/2013 – Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců [online]. [cit. 4. listopadu 2017]

Dostupné z WWW: <https://www.uoou.cz/c-1-2003-monitorovani-elektronicke-posty-a-ochrana-soukromi-a-osobnich-udaju-zamestnancu/ds-2551/archiv=0&p1=2551>.

5. ÚOOÚ: K dodržování povinnosti přijmout a provést bezpečností opatření k ochraně osobních údajů v soukromoprávní sféře [online]. Publikováno dne 21. března 2013 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/k-dodrzovani-povinnosti-prijmout-a-provest-bezpecnosti-opatreni-k-ochrane-osobnich-udaju-v-soukromopravni-sfere/d-1598>.

6. ÚOOÚ: K zabezpečení osobních údajů [online]. Publikováno dne 18. dubna 2013 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/k-zabezpeceni-osobnich-udaju/d-1750/p1=1483>.

7. ÚOOÚ: K zabezpečení osobních údajů v informačním systému (přístupová oprávnění zaměstnanců) [online]. Publikováno dne 18. června 2014 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/k-nbsp-zabezpeceni-osobnich-udaju-v-nbsp-informacnim-systemu-pristupova-opravneni-zamestnancu/d-10895/p1=1483>.

8. ÚOOÚ: Obecné nařízení o ochraně osobních údajů v otázkách a odpovědích [online]. Publikováno dne 25. května 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/obecne-narizeni-o-ochrane-osobnich-udaju-v-otazkach-a-odpovedich/d-23790/p1=3938>.

9. ÚOOÚ: Desatero omylů o obecném nařízení (GDPR) [online]. Publikováno dne 25. května 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/desatero-omylu-o-obecnem-narizeni-gdpr/d-23799/p1=3938>.

10. ÚOOÚ: Změna v hodnocení úrovně právní ochrany biometrických údajů [online]. Publikováno 8. června 2017 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.uoou.cz/zmena-v-nbsp-hodnoceni-urovne-pravni-ochrany-biometrickych-udaju/d-23850>.

11. White & Case: Unlocking the EU General Data Protection Regulation: A practical Handbook on the EU's new Data Protection Law, kapitola 8 [online]. Publikováno dne 25. července 2016 [cit. 4. listopadu 2017]. Dostupné z WWW: <https://www.whitecase.com/publications/article/unlocking-eu-general-data-protection-regulation-practical-handbook-eus-new-data>.

Abstrakt

Cílem této práce je podat vyvážený právní výklad problematiky monitoringu zaměstnanců, a to jak z pohledu práv a právem chráněných zájmů zaměstnavatele, tak z pohledu práva zaměstnanců na soukromí. Sledování zaměstnanců je upraveno zejména v ustanovení § 316 odst. 1 až 3 ZP. Pokud ovšem v rámci monitoringu dochází rovněž ke zpracování osobních údajů zaměstnanců, je nezbytné aplikovat též právní úpravu ochrany osobních údajů. V této práci rozlišuji tzv. jednorázovou či nahodilou kontrolu zaměstnanců prováděnou za účelem ověření dodržování zákazu užívání výrobních a pracovních prostředků zaměstnavatele pro jejich osobní potřebu ve smyslu § 316 odst. 1 ZP a soustavný monitoring zaměstnanců dle § 316 odst. 2 ZP. Dále je nutné se zabývat otázkou, zda též dochází ke zpracování osobních údajů zaměstnanců či nikoli. To znamená, že celkem je v praxi třeba pracovat se čtyřmi typy kontrol/sledování zaměstnanců, z nichž každý má relativně jiný právní režim.

V současné době v oblasti ochrany osobních údajů dochází k největším změnám za posledních více než 20 let; dne 25. května 2018 totiž nabyde účinnosti GDPR. Toto nařízení v plném rozsahu nahradí stávající Směrnici 95/46/ES, která byla do českého práva implementována prostřednictvím ZOOÚ. Osud ZOOÚ není v tuto chvíli zcela jasný; s nejvyšší pravděpodobností však bude zrušen a nahrazen novým zákonem upravujícím pouze dílčí otázky ochrany osobních údajů, jež GDPR svěřuje do kompetence národní právní úpravy. Vzhledem k blížícímu se datu účinnosti GDPR vychází tato práce v oblasti ochrany osobních údajů jak ze ZOOÚ, tak z GDPR.

Tato práce je tematicky rozdělena do tří částí. První část se obecně zabývá zásadami a podmínkami, jež musí zaměstnavatel pro zavedení monitoringu splnit. Jako klíčovou zásadu pro hledání vzájemné rovnováhy práv zaměstnavatele a jeho zaměstnanců je přitom třeba ctít princip proporcionality. Ve druhé části této práce jsou již podrobně rozebrány jednotlivé metody monitoringu včetně dostupné relevantní rozhodovací praxe. U každého z nejčastěji zaváděných sledovacích opatření je zároveň pro ilustraci uvedeno vždy několik návrhů konkrétních scénářů monitoringu. Třetí část této práce se pak zabývá otázkami, jež s monitoringem úzce souvisejí, včetně možnosti

zaměstnavatele vyvodit z výsledků monitoringu důsledky pro zaměstnance a možnosti zaměstnance bránit se proti monitoringu.

Klíčová slova

Monitoring zaměstnanců, GDPR, sledovací opatření, soukromí na pracovišti

Monitoring of Employees and its Methods

Abstract

This thesis intends to offer a balanced legal standpoint on monitoring of employees from the point of view of employer's rights and interests protected by law as well as from the point of view of employees' right to privacy. The surveillance of employees is governed especially by Section 316 (1) through (3) of the Labour Code[248]. However, in case personal data of employees are processed within such monitoring, the personal data protection regulation must be applied as well. This thesis distinguishes between a so-called one-time or random inspection of employees performed within the meaning of Section 316 (1) of the Labour Code for the purpose of checking their observance of ban on using the employer's production and working tools for personal purposes and between continuous monitoring performed under Section 316 (2) of the Labour Code. At the same time, it is necessary to assess whether the employees' personal data are processed as well. Therefore, in practice, four different types of inspections/surveillance of employees have to be distinguished, each of them being governed by slightly different regulation.

Currently, the personal data protection regulation is undergoing the most significant changes in the last more than 20 years; on 25 May 2018, GDPR[249] enters into force. This regulation will replace in full the current Directive 95/46/EC[250] which was implemented into the Czech law by the Personal Data Protection Act[251]. The Personal Data Protection Act's fate is currently unknown; however, most probably it will be abolished and replaced by a new act governing only partial issues of the personal data protection the regulation of which is entrusted by the GDPR into the competence of the

248 Czech Act No. 262/2006 Coll., the Labour Code, as amended.

249 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

250 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

251 Czech Act No. 101/2000 Coll., on Personal Data Protection and Amendment of Certain Acts, as amended.

national legal regulation. With regard to the forthcoming date of entrance of the GDPR into force, this thesis works both with the Personal Data Protection Act and the GDPR.

This thesis is thematically divided into three parts. The first part generally deals with basic principles and conditions to be fulfilled by an employer in order to implement monitoring. The proportionality principle shall be respected as the key principle for the purpose of searching the mutual balance of rights of an employer and its employees. The second part of this thesis describes particular methods of the monitoring in detail, including the available relevant decision-making practice. For the illustration, proposals of specific scenarios of monitoring are included for each one of the most usual methods of monitoring. Finally, the third part of this thesis deals with issues which are closely tied to the monitoring, including the possibility of an employer to conclude certain consequences for an employee from the results of the monitoring and the possibility of an employee to challenge the monitoring.

Keywords

Monitoring of Employees, GDPR, Surveillance Methods, Privacy at Work