UNIVERZITA KARLOVA

Právnická fakulta

Julia Galantseva

Kamerové systémy na pracovišti

Diplomová práce

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

Katedra pracovního práva a práva sociálního zabezpečení (22-KPP)

Datum vypracování práce (uzavření rukopisu) : 27. 11. 2023

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

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 143 088 znaků včetně mezer.

V Praze dne 27. 11. 2023

…….....

Julia Galantseva

Obsah

Úvod 4
1. Pojem a druhy kamerových systémů 6
1.1. Atrapy kamer 7
1.2. Kamerové systémy bez pořizování záznamu a se záznamem 8
2. Podmínky užití kamerových systémů na pracovišti dle zákoníku práce 12
2.1. Právo zaměstnavatele na kontrolu zaměstnanců 12
2.1.1. Kamerové systémy jako prostředek kontroly 13
2.1.2. Kontrola nakládání s pracovními a výrobními prostředky přiměřeným způsobem 14
2.2. Podmínky sledování zaměstnanců 15
2.2.1. Zvláštní povaha činnosti zaměstnavatele 16
2.2.2. Přiměřenost sledování 19
2.2.3. Informační povinnost 21
2.2.4. Skryté sledování 22
3. Atrapy kamer na pracovišti 25
3.1. Rozhodovací praxe inspektorátu práce 25
3.2. Domnělé sledování a právo na ochranu soukromí zaměstnance 27
4. Podmínky užití kamerových systémů na pracovišti dle GDPR 28
4.1. Působnost GPDR a výklad klíčových pojmů 28
4.2. Právní základ ke zpracování osobních údajů 32
4.2.1. Souhlas subjektu údajů 33
4.2.2. Oprávněný zájem zaměstnavatele 34
4.3. Zásady zpracování osobních údajů 37
4.4. Povinnosti zaměstnavatele jakožto správce osobních údajů 41
4.4.1. Informační povinnost 41
4.4.2. Umožnění výkonu práv subjektů údajů 44
4.4.3. Vedení záznamů o činnostech zpracování 49
4.4.4. Posouzení vlivu na ochranu osobních údajů 49
4.4.5. Zajištění zabezpečení zpracování 51
4.4.6. Ohlašování a oznamování bezpečnostních incidentů 54
4.4.7. Jmenování pověřence pro ochranu osobních údajů 55
Závěr 57
Seznam použitých zkratek 59
Seznam použitých zdrojů 60
Příloha 64

Úvod

V dnešní době jsou kamerové systémy téměř neodmyslitelnou součástí každodenního života. Setkáváme se s nimi na každém kroku, a to jak ve veřejných, tak i v soukromých prostorech. Jen v Praze provozoval k roku 2022 Magistrát hl. města Prahy v rámci svého metropolitního systému přes 4500 bezpečnostních kamer. 1038 z nich bylo vybudováno hl. m. Prahou a jejími městskými částmi,[1] ostatní kamery pak náležely jiným veřejnoprávním subjektům, např. Technické správě komunikací, Správě služeb či Městské policii hl. města Prahy.[2] Tato čísla ale nezahrnují kamery nainstalované soukromými subjekty, takže ve skutečnosti obyvatele Prahy každodenně snímá mnohem více kamer.

Kamerové systémy sehrávají v moderní společnosti významnou roli jakožto prostředek ochrany majetku a osob i jako nenahraditelná pomůcka při detekci a vyšetřování trestných činů či přestupků. Videozáznamy pořízené kamerovými systémy často slouží jako spolehlivé důkazní prostředky.

Přes všechnu svou užitečnost představují kamerové systémy významné zásahy do základních práv a svobod fyzických osob, konkrétně do ústavním pořádkem zaručených práv na ochranu soukromí, na ochranu osobnosti a v neposlední řadě také do práva na ochranu osobních údajů.[3] Při instalaci každého kamerového systému tak vzniká potřeba vybalancovat tento zásah do práv snímaných osob se zájmem na ochraně práv provozovatele kamery. To se odráží v právní úpravě, která na národní i evropské úrovni stanoví podmínky zajišťující vyváženost zájmů a vymezující ústavně konformní míru zásahu do práv a svobod dotčených osob.

Výše uvedený střet zájmů nabývá dalšího rozměru při užití kamerových systémů na pracovišti. Dá se říci, že v pracovním prostředí bude sledování pomocí kamer představovat intenzivnější zásah do soukromí dotčených osob. Na pracovišti mohou být zaměstnanci monitorováni po celé trvání jejich pracovní doby a z důvodu vztahu podřízenosti vůči zaměstnavateli se obvykle nemohou sledování z vlastní vůle vyhnout. Dále je u kamerových systémů na pracovišti vyšší pravděpodobnost, že budou snímané osoby na záběrech identifikovatelné. Také z těchto důvodů je právní úprava v této oblasti o něco přísnější –

[1] *Městský kamerový systém hlavního města Prahy* [on-line]. 2022. *Dostupné* z: https://bezpecnost.praha.eu/clanky/kamerovy-system

[2] SLOVÁČEK, P. a HADAČ, T. *Velký bratr na silnicích: Kde všude číhají kamery? A kdo má k záznamům přístup?* [on-line]. 2021. Dostupné z: http://www.1227.cz/aktuality/velky-bratr-na-silnicich-kde-vsude-cihaji-kamery-a-kdo-ma-k-zaznamum-pristup

[3] Viz čl. 7 odst. 1 a 2, čl. 10 odst. 1, 2 a 3 ústavního zákona č. 2/1993 Sb., Listiny základních práv a svobod

zaměstnavatel se musí řídit nejen prameny práva z oblasti ochrany osobních údajů, ale i pracovněprávními předpisy.

Tato diplomová práce se zaměří právě na problematiku monitorování zaměstnanců na pracovišti pomocí kamerových systémů. Cílem práce je zanalyzovat českou právní úpravu sledování zaměstnanců i evropskou právní úpravu ochrany osobních údajů z pohledu kamerových systémů a vymezit jednotlivé podmínky a mantinely užití kamer na pracovišti. Pozornost bude věnována i atrapám kamer z pohledu pracovního práva.

Práce bude rozdělena na čtyři tematické celky. První z nich se bude věnovat zejména definici pojmu „kamerový systém" a rozdělení kamerových systémů na druhy. Dále se první část zabývá otázkou, zda při užití jednotlivých druhů kamerových systémů dochází ke zpracování osobní údajů[4].

Druhá část této práce se zaměří na rozbor právní úpravy sledování zaměstnanců, obsažené v zákoníku práce. V rámci tohoto rozboru bude proveden právní výklad neurčitých právních pojmů pomocí odborné literatury, judikatury, stanovisek či pokynů Úřadu pro ochranu osobních údajů a rozhodovací praxe inspektorátů práce.

Těžištěm třetí části práce je zkoumání zásahů do práv a svobod zaměstnanců, které může představovat užití atrap kamer v pracovním prostředí. V této části se představí také významné novodobé rozhodnutí inspektorátu práce, které prolamuje dosavadní přístup k atrapám kamer.

Čtvrtá a závěrečná část této diplomové práce bude obsahovat analýzu evropské právní úpravy, věnující se ochraně osobních údajů. Zejména budou rozebrány základní pojmy a principy z oblasti ochrany osobních údajů a jednotlivé povinnosti, které zaměstnavateli ze zkoumaných ustanovení vyplývají. Kromě samotného textu právní úpravy bude práce čerpat i z metodik Úřadu pro ochranu osobních údajů i z pokynů či stanovisek Evropského sboru pro ochranu osobních údajů a Pracovní skupiny zřízené dle článku 29.

Jako celek by práce měla nabídnout komplexní vhled do problematiky kamerového sledování zaměstnanců na pracovišti a poskytnout přehled povinností, které by zaměstnavatel měl dodržet jak před započetím monitorování, tak i během něj.

[4] Ve smyslu čl. 4 odst. 2 GDPR

1. Pojem a druhy kamerových systémů

Před započetím analýzy příslušné právní úpravy je třeba si definovat pojem „kamerový systém“ a vymezit jednotlivé druhy kamerových systémů, včetně atrap kamer. Také je nutno určit, na které z vymezených druhů kamerových systémů dopadá právní úprava na ochranu osobních údajů.

Definice kamerového systému

Ačkoliv je v českém právním řádu problematika monitorování osob upravena v řadě právních předpisů, samotný pojem „kamerový systém“ není v současné legislativě definován.

Zákonodárce pojem „kamerový systém“ zmiňuje pouze v rámci výčtů bezpečnostních a technických opatření, která jsou vyžadována pro zajištění provozu některých rizikových zařízení.[5]

Kamerové sledování je právní úpravou regulováno spíše implicitně, např. v rámci stanovení zákonných podmínek pro „sledování“, které najdeme mj. v § 316 odst. 2 zákoníku práce.

Definici „kamerového systému“ lze nalézt v *Komentáři k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů*, vydaném v roce 2006 Úřadem pro ochranu osobních údajů. Úřad v tomto dokumentu vymezuje kamerový systém jako „*automaticky provozovaný stálý technický systém umožňující pořizovat a uchovávat zvukové, obrazové nebo jiné záznamy ze sledovaných míst*.“[6]

Za zmínění stojí také definice obsažená v *Pokynech 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* vydaných Evropským sborem pro ochranu osobních údajů.[7] Pokyny 3/2019 neužívají pojem „kamerový systém“, definují však významově obdobný pojem „dohledový videosystém“.[8] „Dohledový videosystém“ dle Pokynů 3/2019 „*sestává z analogových a digitálních zařízení a softwaru za účelem zachycení snímků scény, zpracování snímků a jejich*

[5] § 24d písm. b) zákona č. 167/1998 Sb., o návykových látkách; § 22 společně s § 10 odst. 4 zákona č. 307/2013 Sb., o povinném značení lihu

[6] Úřad pro ochranu osobních údajů. *Příloha č. 2 k tiskové zprávě z 26. 1. 2006, Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů*. [on-line]. 2006. Dostupné z: https://old.uoou.cz/tiskova-zprava-26-1-2006/ds-1217/archiv=0&p1=1017

[7] Evropský sbor pro ochranu osobních údajů byl zřízen obecným nařízením o ochraně osobních údajů. Jedná se o nezávislý subjekt, který se snaží harmonizovat uplatňování předpisů na ochranu osobních údajů napříč Evropskou unií.

[8] angl. „video surveillance systém“ („VSS“)

zobrazení pracovníkovi.“[9] Pokyny 3/2019 dále vymezují i jednotlivé technické prvky „dohledového videosystému“.

Druhy kamerových systémů

V současnosti využívané kamerové systémy lze členit na jednotlivé druhy podle různých kritérií, např. dle jejich konstrukčního provedení, typu snímaní či typu zpracování obrazu.[10]

Pro účely této práce bude nicméně rozhodující pouze dělení relevantní z právního hlediska[11] na kamerové systémy s pořizováním záznamu a kamerové systémy bez pořizování záznamu. „Záznam“ pro účely tohoto dělení lze definovat jako „*technický způsob uchování vizuální nebo zvukové informace, který více či méně věrně reprodukuje osobní zjev či projev, který fyzická osoba v minulosti učinila*“, přičemž takový zaznamenaný projev musí být zároveň „*opakovaně reprodukovatelný*“.[12]

Jako jednotlivou kategorii je třeba zmínit i kamerové systémy vybavené možností snímat biometrické charakteristiky osob, které dle Úřadu představují velmi vysokou míru narušení práv a zájmů dotčených osob.[13]

V této práci bude věnována pozornost i kategorii, která definici kamerových systémů nenaplňuje, konkrétně falešným bezpečnostním kamerám, tzv. atrapám kamer.

1.1. Atrapy kamer

Atrapami kamer se rozumí napodobeniny bezpečnostních kamer, případně vypnuté bezpečnostní kamery, které mají případné pachatele od protiprávního jednání odradit pouhým vzbuzením dojmu kamerového sledování. Atrapy kamer zpravidla nejsou funkčním elektronickým zařízením[14] a nejsou tudíž schopny jakéhokoli obrazového či jiného snímání.[15]

---

[9] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 30-31.
[10] *Rozdělení a druhy bezpečnostních kamer CCTV* [on-line]. Dostupné z: http://www.hlidacikamery.cz/druhy-kamer/
[11] Konkrétně z hlediska právní úpravy ochrany osobních údajů.
[12] JANEČKOVÁ, E. a BARTÍK, V. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde, 2011. Praktická právnická příručka. ISBN 978-80-7201-850-5. S. 18.
[13] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 19-20.
[14] Některé atrapy jsou vybaveny např. blikající LED diodou, která má simulovat snímání.
[15] To ovšem neznamená, že prostřednictvím atrap nemůže dojít k újmě na právech a svobodách osob.

1.2. Kamerové systémy bez pořizování záznamu a se záznamem

Monitorování pomocí kamerového systému neumožňujícího pořizovat záznam[16] nebylo v minulosti Úřadem považováno za zpracování osobních údajů ve smyslu ustanovení § 4 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů.[17] To mimo jiné znamenalo, že se na kamerové systémy bez pořizování záznamu nevztahovaly povinnosti vyplývající z tehdejších předpisů na ochranu osobních údajů, např. že tyto kamerové systémy nebylo nutno oznamovat Úřadu.[18]

Úřad toto rozlišení poprvé vymezil ve svém *Stanovisku č. 1/2006 – Provozování kamerového systému z hlediska zákona o ochraně osobních údajů*, kde uvedl, že *„Provozování kamerového systému je považováno za zpracování osobních údajů, pokud je vedle kamerového sledování prováděn záznam pořizovaných záběrů, nebo jsou v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Samotné kamerové sledování fyzických osob není zpracováním osobních údajů podle zákona č. 101/2000 Sb.“*[19]

Tento výklad Úřad potvrdil i po deseti letech, ve svém *Stanovisku č. 1/2016 - Umístění kamerových systémů v bytových domech*. V tomto stanovisku Úřad hned v několika instancích zdůrazňuje, že o zpracování osobních údajů se jedná v případě kamerového sledování se současným pořizováním záznamu, např. v odst. 1 stanoviska: „[ú]*řad pro ochranu osobních údajů (dále jen „Úřad“) vydává toto stanovisko vztahující se ke zpracování osobních údajů prostřednictvím kamery se záznamem instalované v bytovém domě* […]“ či v jeho odst. 2: „[č]*astými důvody pro zpracování osobních údajů – pořizování záznamů kamerovými systémy* […]“.[20]

Toto rozlišení nebylo po dobu platnosti zákona o ochraně osobních údajů vážně zpochybněno a utvrdil jej mj. ve své judikatuře i Nejvyšší správní soud.[21] Úřad sice uspořádal dne

---

[16] Také např. „on-line monitorování“ či „monitorování v reálném čase“.
[17] Zákon o ochraně osobních údajů byl derogován dne 24. 04. 2019 zákonem č. 110/2019 Sb. v návaznosti na přijetí obecného nařízení o ochraně osobních údajů.
[18] Srov. § 16 zákona o ochraně osobních údajů.
[19] Úřad pro ochranu osobních údajů. *Stanovisko č. 1/2006 - Provozování kamerového systému z hlediska zákona o ochraně osobních údajů* [on-line]. 2006. Dostupné z: https://old.uoou.cz/files/stanovisko_2006_1.pdf
[20] Úřad pro ochranu osobních údajů. *Stanovisko č. 1/2016 - Umístění kamerových systémů v bytových domech* [on-line]. 2016. Dostupné z: https://old.uoou.cz/stanovisko-c-1-2016-umisteni-kamerovych-systemu-v-bytovych-domech/d-18866
[21] Např. rozsudek Nejvyššího správního soudu ze dne 8. listopadu 2011, č. j. 2 As 45/2010- 68, ve kterém Nejvyšší správní soud uvádí následující: „*Pokud je kamerové snímání prováděno nikoli náhodně, ale systematicky a je-li z něho prováděn záznam, umožňující následně provést identifikaci osoby…jde mimo jakoukoli pochybnost o zpracování osobních údajů*“.

14. června 2016 diskuzi na téma, zda je „*možné, vhodné a efektivní i on-line sledovací systémy chápat jako nástroje pro zpracování osobních údajů*“, také z důvodů několika případů narušení zabezpečení on-line kamerových systémů a následného zveřejnění snímků na internetu. Účastníci diskuze se převážně shodli, že i pro oblast on-line kamerových systémů je nutno nastavit určitá pravidla a neponechat je zcela bez regulace.[22] Není však známo, že by tato diskuze přispěla ke změně tehdejšího právního názoru Úřadu.

Odlišný názor byl v rámci evropského práva prezentován až po vstupu obecného nařízení o ochraně osobních údajů v platnost, a to v *Pokynech 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* vydaných Evropským sborem pro ochranu osobních údajů.

Sbor ve svých Pokynech 3/2019 výslovně uvádí několik činností, které nepokládá za zpracování osobních údajů. Jsou jimi např. kamerové sledování, prováděné z vysokých výšek (pokud v rámci takového sledování nelze identifikovat konkrétní fyzické osoby) či videodohled v rámci osobní a domácí činnosti[23]. O kamerovém sledování bez pořizování záznamu (pro označení kterého Sbor užívá pojem „monitorování v reálném čase“) se však v této souvislosti vůbec nezmiňuje.

Naopak kupříkladu v bodě 92 Pokynů 3/2019 Sbor jasně vymezuje dobu, po kterou probíhá „monitorování v reálném čase“ jako časový okamžik, ve kterém ke zpracování osobních údajů dochází, viz „[…] *pokud nejsou žádné údaje ukládány nebo předávány jakýmkoli způsobem, pak jakmile uplyne okamžik monitorování v reálném čase, může správce poskytnout pouze informaci o tom, že se žádné osobní údaje již nezpracovávají*“.[24]

Dále lze poukázat i na bod 29 Pokynů 3/2019, ve kterém Sbor hovoří o „monitorování v reálném čase“ jako o jednom ze způsobů kamerového sledování, který lze zvolit jako alternativu vůči ukládání záznamů, ale pouze pokud je to v dané situaci vhodné – uvádí totiž i příklad, kdy by monitorování v reálném čase mohlo být oproti pořizování záznamů dokonce invazivnější: „*např. pokud někdo neustále sleduje obrazovku, může to být rušivější než v případě, že monitor vůbec neexistuje a materiály jsou uloženy přímo v černé skříňce*“.[25] Ve smyslu definice zpracování osobních údajů dle čl. 4 odst. 2 GDPR lze on-line monitorování považovat např. za „šíření nebo

[22] Úřad pro ochranu osobních údajů. *Kulatý stůl k využívání on-line kamer a dalších sledovacích zařízení* [on-line]. 2016. Dostupné z: https://old.uoou.cz/kulaty-stul-k-vyuzivani-on-line-kamer-a-dalsich-sledovacich-zarizeni/d-20310/p1=1099

[23] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 7-8.

[24] Tamtéž. S. 22.

[25] Tamtéž. S. 11.

jakékoliv jiné zpřístupnění“, jelikož v procesu takového monitorování jsou osobní údaje snímaných subjektů zpřístupněny osobám, které sledují on-line přenos.

V kontextu GDPR a Pokynů 3/2019 zřejmě došlo k názorovému posunu Úřadu, který již nepovažuje on-line monitorování za činnost, která není zpracováním osobních údajů, když ve svém vodítku *K provozování kamer* z roku 2022 uvádí, že „[s]*kutečnost, že v rámci kamerového systému nedochází k ukládání záznamů například na harddisk či jiné záznamové médium, tedy neznamená, že je takové zpracování osobních údajů skrze kamerové systémy mimo působnosti GDPR.*“ Za zpracování osobních údajů ve stejném dokumentu považuje i „*šíření obrazového nebo audiovizuálního signálu monitorovaného veřejného prostoru obsahujícího údaje využitelné k identifikaci fyzických osob*“.[26]

V čl. 2.3 *Návrhu Metodiky ke kamerovým systémům* Úřadu z 24. dubna 2023 Úřad dále utvrzuje výše zmíněný názor a výslovně uvádí, že „*Kamerový systém využívaný v režimu on-line představuje zpracování osobních údajů, jak vyplývá například z § 29 Pokynů EDPB 3/2019*.“[27] V článku 2.2 Návrhu metodiky také přichází s možným dělením kamerových systémů dle rozlišení přenášeného obrazu do šesti kategorií, a to monitorování[28], zjištění[29], pozorování, rekognoskace, identifikace a prozkoumání. V případě kamerových systémů s úrovní rozlišení odpovídající kategoriím monitorování a zjištění[30] dle Úřadu ke zpracování osobních údajů nedochází, jelikož v tomto rozlišení nelze bez vynaložení nepřiměřeného úsilí identifikovat jednotlivé snímané osoby. Následně Úřad podotýká, že užití kamerových systémů s rozlišením spadajícím do zbylých čtyř kategorií již představuje zpracování osobních údajů bez ohledu na to, jestli jsou provozovány se záznamem či bez záznamu.[31]

Dle současného názoru Úřadu tak právní předpisy z oblasti ochrany osobních údajů dopadají na oba výše vymezené druhy kamerových systémů.[32] V případě rozsahu působnosti GDPR se však mohou objevit určité rozdíly. Kupříkladu jelikož kamerové systémy bez záznamu

---

[26] Úřad pro ochranu osobních údajů. *K provozování kamer a kamerových systémů* [on-line]. 2022. Dostupné z: https://old.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=29535&n=k%2Dprovozovani%2Dkamer%2Da%2Dkamerovych%2Dsystemu&p1=1099

[27] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 5.

[28] Kamerové systémy s rozlišením obrazu více než 80 mm na pixel.

[29] Kamerové systémy s rozlišením obrazu více než 40 mm na pixel.

[30] Tyto kategorie kamerových systémů mohou dle Úřadu být využity v on-line systémech za účelem řešení mimořádných událostí, kdy se vyžaduje rychlá reakce ze strany monitorující osoby.

[31] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 4.

[32] Pokud stupeň rozlišení snímaného obrazu umožňuje identifikovat jednotlivé osoby.

osobní údaje neukládají, subjekty údajů nemohou uplatnit svá práva na výmaz, opravu či na přístup ke svým osobním údajům.[33]

Také lze polemizovat, zda ke zpracování osobních údajů dochází i ve chvíli, kdy záběry z kamerového systému bez záznamu nesleduje žádná osoba. V takovém okamžiku ke zpracování osobních údajů nejspíše nedochází, což lze dovodit z čl. 2.3 Návrhu metodiky, v němž Úřad vymezuje operace zpracování probíhající při použití kamerového systému bez záznamu jako „*Prohlížení on-line záběrů z kamerového systému (snímaní, přenos, zobrazení).*“[34] Lze si tak představit teoretickou situaci, kdy by po celou dobu fungování kamerového systému bez záznamu nebyl přenášený obraz nikým sledován a v žádném okamžiku by tak nedocházelo ke zpracování osobních údajů. V takovém případě je možné usoudit, že by se povinnosti vyplývající z GDPR na tento kamerový systém nevztahovaly.

[33] Srov. čl. 15-17 GDPR.
[34] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 5.

2. Podmínky užití kamerových systémů na pracovišti dle zákoníku práce

S ohledem na výhody kamerových systémů není divu, že se dnes velmi často instalují i na pracovišti,[35] kde jsou užívány většinou za účelem ochrany majetku zaměstnavatele a ochrany života a zdraví zaměstnanců i třetích osob.

V momentě umístění kamerového systému na pracoviště nicméně dochází ke střetu práv dvou významných aktérů. Kamerový systém sice umožňuje efektivnější ochranu zájmů zaměstnavatele, tj. jeho majetku a jeho zájmu na řádném výkonu pracovních povinností zaměstnanci, na druhou stranu představuje i významný zásah do práv zaměstnanců, a to především do jejich ústavně zaručeného práva na soukromí.

Tento střet zájmů upravuje ustanovení § 316 zákoníku práce, které se věnuje podmínkám a rozsahu užití kontrolních mechanismů na pracovišti. Toto ustanovení stanoví obecná pravidla pro zavádění těchto mechanismů, mezi které řadí i otevřené a skryté sledování zaměstnanců na jejich pracovištích.

2.1. Právo zaměstnavatele na kontrolu zaměstnanců

Zákoník práce přiznává zaměstnavateli právo na kontrolu zaměstnanců, které je upraveno mj. v § 316 ZPr. Toto ustanovení, které tvoří jediný paragraf Hlavy VIII. 13. části zákoníku práce s názvem *Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance*, se věnuje právě střetu těchto dvou skupin práv. Toto je zřejmé i ze stručné důvodové zprávy k tomuto ustanovení.[36]

Samotné právo na kontrolu je přímo zakotveno v § 316 odst. 1 ZPr. Věta první tohoto ustanovení se věnuje ochraně majetkových zájmů zaměstnavatele tak, že stanovuje zaměstnancům zákaz užívání výrobních a pracovních prostředků zaměstnavatele bez jeho souhlasu;[37] věta druhá pak zní: „*Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.*“ Ze znění věty druhé tohoto ustanovení vyplývá, že zákonodárce v tomto případě právo kontrolovat vztahuje pouze na kontrolu nakládání s výrobními a pracovními prostředky.

---

[35] Pojem „pracoviště“ je v této práci brán v souladu s jeho vymezením Nejvyšším soudem v jeho rozsudku ze dne 26. 11. 2015, sp. zn. 21 Cdo 4596/2014 jako „*určitý konkrétní prostor, ve kterém zaměstnanec fakticky vykonává dohodnutou práci, popřípadě prostor, kde se nachází jeho kancelář*“.

[36] Srov. *Důvodová zpráva k zákonu č. 262/2006 Sb., zákoník práce.,* Sněmovní tisk 1153/0.

[37] Úplné znění věty první § 316 odst. 1 zákoníku práce: „*Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení.*“

Nicméně následující § 316 odst. 2 ZPr, který upravuje podmínky zavedení kontrolních mechanismů na pracovišti, se věnuje úpravě i takových kontrolních mechanismů, které naprosto nesouvisí s kontrolou zákazu dle § 316 odst. 1 věty první ZPr, např. kontrole listovních zásilek adresovaných zaměstnanci.[38] Z toho pak lze dovodit, společně s již zmíněným názvem Hlavy VIII. 13. části ZPr, že se § 316 ZPr jako celek nevěnuje pouze právu zaměstnavatele na kontrolu zaměstnanců ve smyslu ust. § 316 odst. 1 ZPr, nýbrž kontrole zaměstnanců za účelem ochrany majetkových zájmů zaměstnavatele v širším smyslu. Taková kontrola může zahrnovat např. kontrolu dodržování pracovních povinností či kontrolu nakládání s majetkem zaměstnavatele, který nespadá pod definici § 316 odst. 1 věty první ZPr, ve zkratce tedy kontrolu všech jednání, které by mohly ohrozit majetkové zájmy zaměstnavatele.[39]

Mimo Hlavu VIII. 13. části ZPr se kontrole zaměstnanců v zákoníku práce věnují i některá další ustanovení, jako např. § 302 písm. a), které stanoví vedoucím zaměstnancům povinnost kontrolovat své podřízené nebo § 248 odst. 2, který opravňuje zaměstnavatele „*z důvodu ochrany majetku* […] *v nezbytném rozsahu provádět kontrolu věcí, které zaměstnanci k němu vnášejí nebo od něho odnášejí, popřípadě provádět prohlídky zaměstnanců*“.[40] Tato ustanovení však nejsou relevantní z pohledu kontroly zaměstnanců pomocí kamerových systémů.

2.1.1. Kamerové systémy jako prostředek kontroly

Okruh možných prostředků kontroly zaměstnanců vymezuje ustanovení § 316 odst. 2 zákoníku práce taxativně, a to jako otevřené nebo skryté sledování, odposlech a záznam telefonických hovorů zaměstnance, kontrolu elektronické pošty a kontrolu listovních zásilek adresovaných zaměstnanci.

Kamerové systémy z tohoto výčtu lze podřadit pouze pod pojem „sledování“, které je v trestněprávních předpisech právního řádu vymezeno jako „*získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky*“.[41] V pracovněprávním kontextu je tuto definici možno použít jen z části, jelikož v ust. § 316 odst. 2

[38] MORÁVEK, J. § 316 [Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance]. In: PICHRT, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.
[39] Tamtéž.
[40] JANEČKOVÁ, E. a BARTÍK, V. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde, 2011. Praktická právnická příručka. ISBN 978-80-7201-850-5. S. 33.
[41] § 158d odst. 1 zákona č. 141/1961 Sb., trestního řádu

ZPr je sledování přímo specifikováno jako otevřené nebo skryté. U „otevřeného sledování“ tedy nelze uplatnit část výše uvedené definice, která stanoví požadavek „utajení“.

Monitorování kamerovým systémem tuto (upravenou) definici splňuje a lze ho tedy považovat za sledování. Otevřenost či skrytost sledování pak u kamerových systémů může vyplývat z technického způsobu provedení sledování (tj. z viditelnosti kamer) a ze stupně informovanosti sledovaných subjektů.

2.1.2. Kontrola nakládání s pracovními a výrobními prostředky přiměřeným způsobem

Ustanovení § 316 odst. 1 zákoníku práce, které zaměstnavateli přiznává právo na kontrolu zaměstnaneckého užívání výrobních a pracovních prostředků, stanoví ve větě druhé pouze podmínku provádění kontroly „přiměřeným způsobem“. Předmětné ustanovení na rozdíl od odst. 2 stejného paragrafu nevymezuje možné způsoby provádění kontroly, ani dále nijak nekonkretizuje „přiměřený způsob“. Výklad tohoto pojmu tak lze hledat v odborné literatuře či v judikatuře.

Dle Vidrny a Koudelky je možné pojem „přiměřený způsob kontroly“ vyložit s ohledem na finanční hledisko. Uvádí, že „*způsob (forma, charakter, prostředky) kontroly má být v rozumném poměru k těm hodnotám, které prostřednictvím něho mají být chráněny. Určitým vodítkem proto může být například finanční hodnota pořízení (anebo náklady provozu) výrobních a pracovních prostředků zaměstnavatele, včetně výpočetní techniky a jeho telekomunikačního zařízení.*“[42]

Nezávisle na výše prezentovaném výkladu se tímto pojmem zabývá i Nejvyšší soud ve svém rozsudku sp. zn. 21 Cdo 1771/2011. V tomto rozhodnutí vymezuje možná kritéria, ke kterým může přihlížet soud při rozhodování, zda byl požadavek „přiměřeného způsobu kontroly“ naplněn: „*zda šlo o kontrolu průběžnou či následnou, k její délce, rozsahu, k tomu, zda vůbec a do jaké míry omezovala zaměstnance v jeho činnosti, zda vůbec a do jaké míry zasahovala také do práva na soukromí zaměstnance apod.*“ Nejvyšší soud dále zmiňuje, že předmětem přiměřené kontroly podle § 316 odst. 1 ZPr může být „*toliko zjištění, zda zaměstnanec porušil zákonem stanovený absolutní zákaz*“. Naráží tak na skutečnost, že kontrola ve větším rozsahu (např. obecná kontrola plnění pracovních povinností) by nebyla ve smyslu § 316 odst. 1 ZPr přiměřená. Zároveň

[42] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců*. V Praze: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7. S. 27.

upozorňuje na možnost zaměstnavatele udělit souhlas s užitím jeho výrobních a pracovních prostředků pro osobní potřeby zaměstnanců, když považuje za přiměřenou pouze kontrolu takových prostředků, k jejichž osobnímu užívání zaměstnavatel souhlas neudělil: „*půjde tedy jen o kontrolu nedodržení těch povinností, jež nebyly zaměstnavatelem vyloučeny nebo zmírněny.“* Na závěr Nejvyšší soud zdůrazňuje, že výklad „přiměřeného způsobu“ kontroly nemůže být natolik svazující, aby právo zaměstnavatele na kontrolu zaměstnance úplně zaniklo tím, že by ho nemohl realisticky vymáhat: „*Zároveň je třeba mít na zřeteli, že, má-li zaměstnanec zakázáno užívat majetek zaměstnavatele pro svou osobní potřebu a zaměstnavatel má právo kontrolovat dodržování tohoto zákazu, musí mít zaměstnavatel také možnost nějakým způsobem tuto kontrolu realizovat a získat případně důkaz o nedodržování uvedeného zákazu.*“[43]

V případě kontroly užívání výrobních a pracovních prostředků pomocí kamerového systému by ale zaměstnavateli nestačilo splnit pouze kritérium „přiměřenosti“ dle § 316 odst. 1 ZPr. Jak už bylo nastíněno v předchozí kapitole, kamerové systémy spadají pod definici „sledování“ a jsou tak jedním z kontrolních mechanismů, na které dopadají omezení vyplývající z § 316 odst. 2 a 3 ZPr. Výjimkou by mohl být případ, kdy by i přes použití kamerových systémů ke kontrole zákazu dle § 316 odst. 1 ZPr nedocházelo k jakémukoliv narušování soukromí zaměstnanců.[44]

2.2. Podmínky sledování zaměstnanců

Možnost sledování zaměstnanců na pracovišti je omezena podmínkami, které vyvstávají z § 316 odst. 2 a 3 zákoníku práce. Dle § 316 odst. 2 ZPr „*Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci*.“

Výše uvedené omezení obsažené v § 316 odst. 2 zákoníku práce stanoví plošný zákaz narušování soukromí zaměstnance na pracovišti i ve společných prostorách prostřednictvím taxativně vyjmenovaných kontrolních mechanismů, mezi které patří i „sledování“, jež lze provozovat pomocí kamerových systémů. Zákoník práce zde upravuje právo na ochranu soukromí

[43] Rozsudek Nejvyššího soudu ze dne 16. 08. 2012, sp. zn. 21 Cdo 1771/2011

[44] MORÁVEK, J. § 316 [Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance]. In: PICHRT, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.

zaměstnanců, které v předchozí právní úpravě[45] nebylo přímo zakotveno. Důvodová zpráva k zákoníku práce v této souvislosti uvádí, že se nedostatek tehdejší právní úpravy v oblasti ochrany soukromí zaměstnanců musel dohánět „*výkladem za použití obecných ústavních východisek vyplývajících z Listiny základních práv a svobod a za použití § 7 odst. 2 dosavadního zákoníku práce o postupu podle zásady dobrých mravů.*“[46]

V případě § 316 odst. 2 ZPr se jedná o kogentní normu, kterou nelze prolomit ani se souhlasem zaměstnance[47]. Zaměstnavatel tak vždy musí dodržet zákonné podmínky kontroly, které zákoník práce formuluje jako „závažné důvody, spočívající ve zvláštní povaze činnosti zaměstnavatele“. Jedná se opět o relativně neurčitý pojem, jehož výkladu se věnuje odborná literatura, judikatura i Státní úřad inspekce práce a v praxi také oblastní inspektoráty práce.

2.2.1. Zvláštní povaha činnosti zaměstnavatele

Morávek zdůrazňuje, že před výkladem pojmu „zvláštní povaha činnosti zaměstnavatele“ je nutno rozlišit, zda míří na činnost zaměstnavatele v širším smyslu či v užším smyslu. Činností v širším smyslu rozumí předmět činnosti zaměstnavatele zapsaný ve veřejném rejstříku, za činnost zaměstnavatele v užším smyslu pak označuje „*dílčí činnosti realizované u zaměstnavatele, jejichž prostřednictvím se zajišťuje naplnění činnosti zaměstnavatele v širokém smyslu. Může se jednat např. o „vedení účetnictví, spravování skladových zásob, prodej zboží atp.“*.“ Podle Morávka je v případě výkladu předmětného pojmu vhodné zkoumání pouze činnosti zaměstnavatele v užším smyslu, opak by dle něj vedl k „*nedůvodné restrikci hypotézy právní normy*.“[48]

Dále se dá diskutovat o tom, jaké povahy činnosti zaměstnavatele v užším smyslu je možno považovat za „zvláštní“. Státní úřad inspekce práce ve svém informačním letáku k ustanovení § 316 ZPr zdůrazňuje, že „*hodnocení je vždy třeba vztáhnout ke konkrétnímu pracovišti a konkrétnímu zaměstnavateli.*“ Zmiňuje však, že závažné důvody dle § 316 odst. 2 ZPr nenastávají „*při výrobě běžných výrobků nebo při poskytování běžných služeb.*”[49]

---

[45] Srov. zákon č. 65/1965 Sb., zákoník práce.
[46] *Důvodová zpráva k zákonu č. 262/2006 Sb., zákoník práce.,* Sněmovní tisk 1153/0
[47] JANEČKOVÁ, E. a BARTÍK, V. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde, 2011. Praktická právnická příručka. ISBN 978-80-7201-850-5. S. 32-33.
[48] MORÁVEK, J. § 316 [Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance]. In: PICHRT, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.
[49] Státní úřad inspekce práce. *Ochrana osobních práv zaměstnanců a ochrana majetkových zájmů zaměstnavatele.* 2019. [on-line]. Dostupné z: https://www.suip.cz/documents/20142/43720/ochrana_os_2019.pdf/6e6c9012-7616-40f3-1fef-b443c682e94a

Městský soud v Praze pak ve svém rozhodnutí sp. zn. 5 A 107/2013 – 38 považuje kontrolu dle § 316 odst. 2 nejen za prostředek ochrany majetku zaměstnavatele. Konstatuje, že „*kamerový systém neslouží zaměstnavatelům pouze k ochraně majetku a kontrole zaměstnanců, nýbrž především k ochraně zaměstnanců*." Požadavek na „zvláštní povahu činnosti" vykládá jako činnosti, které jsou mimořádně nebezpečné, s tím, že za příklad uvádí „*nakládání s vysoce nebezpečnými chemikáliemi či s vysokými finančními částkami*".[50] Tento výklad částečně potvrzuje i Nejvyšší správní soud ve svém rozsudku sp. zn. 10 As 245/2016 – 41, když označuje „některé vysoce nebezpečné provozy" za situace „*na které pamatuje § 316 odst. 2 zákoníku práce hovořící o zvláštní povaze činnosti zaměstnavatele.*"[51] Stejný přístup sdílí i Kottnauer, který za závažný důvod ke sledování zaměstnanců považuje např. „*prác*[i] *zaměstnanců s utajovanými informacemi, nebezpečnými chemickými látkami nebo jejich prác*[i] *výrobě zbraní, munice nebo výbušnin, popř. manipulace s nimi.*"[52] Vidrna a Koudelka ve svém výkladu míří podobným směrem a pod pojmem „zvláštní povaha činnosti" si představují „*konkrétní pracoviště, kde existuje reálné riziko ohrožení života a zdraví, zpronevěra větších finančních částek, škoda značného rozsahu například při nedodržení technologických postupů výroby apod.*"[53]

Inspektoráty práce ve své rozhodovací činnosti pojem vykládají také spíše restriktivně. V jednom z rozhodnutí oblastního inspektorátu práce lze nalézt vymezení pojmu jako „*např. provozování strojů či technologií, které mohou potenciálně způsobit škodu, ať už na zdraví zaměstnanců či třetích osob nebo majetku. Jednalo by se např. o vysoce specializovaná pracoviště, kde chybný úkon znamená riziko většího ohrožení*."[54]

Existují i odlišná stanoviska, dle kterých nelze „zvláštní povahu činnosti zaměstnavatele" vykládat v souladu s výše prezentovanými názory pouze jako nebezpečné činnosti. Kupříkladu Výzkumný ústav bezpečnosti práce ve své publikaci z roku 2020 uvádí, že „[n]*ení však možno být zajedno s názory, podle nichž náleží právo kontroly jen zaměstnavatelům, u kterých jsou vykonávány činnosti zvlášť nebezpečné nebo mimořádně ohrožující, např. zaměstnavatelům s provozy, kde se pracuje s výbušninami, zaměstnavatelům provozujícím jaderné elektrárny apod.*" Tento právní názor dle Ústavu podporuje i *Stanovisko 8/2001* Pracovní skupiny zřízené podle

[50] Rozsudek Městského soudu v Praze ze dne 18. 10. 2016, sp. zn. 5 A 107/2013 - 38
[51] Rozsudek Nejvyššího správního soudu ze dne 20. 12. 2017, sp. zn. 10 As 245/2016 - 41
[52] KOTTNAUER, A. § 316. In: KOTTNAUER, A. *Zákoník práce: komentář*. Praha: Leges, 2012. Komentátor. ISBN 978-80-87576-08-3.
[53] VIDRNA, J. a KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců*. V Praze: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7. S. 122.
[54] Viz Příkaz Oblastního inspektorátu práce pro hlavní město Prahu pod sp. zn. S3-2020-49, který tvoří Přílohu č. 1 této diplomové práce

článku 29,[55] „*podle něhož je možno za předpokladu splnění stanovených podmínek přiznat právo kontroly jakémukoliv zaměstnavateli*." [56]

Janečková a Bartík v souladu s výše představeným názorem kladou důraz spíše na citlivou, ne nutně nebezpečnou povahu činnosti zaměstnavatele, když spekulují, že zákonodárcem mohly být myšleny „*takové činnosti zaměstnavatele, kde je třeba dbát zvýšených nároků na chování zaměstnanců (např. vzhledem k ochraně utajovaných skutečností, povinnosti mlčenlivosti, ochraně obchodního tajemství, vyšších majetkových hodnot, know how apod.).*"[57] Podobný výklad, zaměřený na zvýšené povinnosti zaměstnanců najdeme i u Morávka, který za zvláštní činnost považuje „*za určitých okolností* [...] *činnost vrcholového manažera, který disponuje širokými rozhodovacími kompetencemi ve vztahu k majetku zaměstnavatele a dispozičními právy k bankovním účtům, stejně tak jako o činnost zaměstnance ve výrobě, který má přístup k jádru obchodního tajemství (originální receptuře atp.) zaměstnavatele.*".[58]

Úřad pro ochranu osobních údajů sice k problematice nevydal žádné stanovisko či vodítko, v jednom z jeho rozhodnutí však lze dohledat negativní vymezení pojmu. Uvádí, že za zvláštní povahu činnosti v žádném případě nelze „*považovat činnost vykonávanou na recepci nebo přepážkách městské části, kde se například vydávají občanské průkazy*."[59]

Z výše uvedených protichůdných názorů nelze dovodit jasný výklad zkoumaného pojmu „zvláštní povaha činnosti zaměstnavatele" a ani jednoznačná kritéria, která by mohla pomoci zúžit okruh těchto činností, také z důvodu, že se jedná většinou o nezávazné výklady. Výklad nalezený v judikatuře je pouze částečný a nebyl již dále rozveden či potvrzen jinými soudními rozhodnutími. Výše uvedená rozporuplnost výkladů se jeví jako problematická, jelikož neurčitost zkoumaného pojmu a absence jasných mantinelů interpretace soustřeďuje moc v rukou správních orgánů, jako jsou inspektoráty práce a ponechává jím až moc prostoru k výkladu, což může narušit princip

[55] Stanovisko 8/2001 ke zpracování osobních údajů v souvislosti se zaměstnáním, vypracované speciálním kolegiem expertů ustanoveným na základě ustanovení čl. 29 dnes již derogované 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.

[56] Výzkumný ústav bezpečnosti práce. *Odraz Obecného nařízení o ochraně osobních údajů v oblasti bezpečnosti a ochrany zdraví při práci a ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance.* 2020. [on-line]. Dostupné z: https://vubp.cz/soubory/produkty/publikace-ke-stazeni/odraz-gdpr-v-oblasti-bezpecnosti-a-ochrany-zdravi-pri-praci-a-ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance.pdf

[57] JANEČKOVÁ, E., BARTÍK, V. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde, 2011. Praktická právnická příručka. ISBN 978-80-7201-850-5. S. 33.

[58] MORÁVEK, J. § 316 [Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance]. In: PICHRT, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.

[59] Příkaz Úřadu pro ochranu osobních údajů ze dne 6. 2. 2018, čj. UOOU-00063/18-3. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=54627

právní jistoty, jehož součástí je legitimní předvídatelnost správních postupů. K tomuto problému přispívá i relativní nedostupnost předchozích rozhodnutí inspektorátů práce,[60] která lze získat pouze prostřednictvím žádostí dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, přičemž takové poskytnutí informací může být spojeno s vysokými poplatky.

2.2.2. Přiměřenost sledování

Podmínka „zvláštní povahy činnosti zaměstnavatele" nicméně není jediným zákonným omezením monitorování zaměstnanců dle § 316 odst. 2 ZPr. Zaměstnavatel musí splňovat i kritérium „závažného důvodu", které je dle Morávka nutno vykládat „*tak, že i když se jedná o zvláštní povahu činnosti, musí z hlediska testu přiměřenosti zájem zaměstnavatele převážit nad chráněnými zájmy (zejména soukromím) na straně zaměstnance, přičemž v rámci vážení bude třeba hodnotit i kritérium potřebnosti a vhodnosti. Respektován musí být také princip nezbytnosti. Při uvažování o zvoleném způsobu kontroly je z hlediska jednotlivých dílčích kritérií testu přiměřenosti (vhodnost, nutnost, přiměřenost) třeba posoudit zvolený prostředek a způsob kontroly jako celek.*"[61] Dle Nejvyššího správního soudu musí být kontrola „*přiměřená cíli a musí narušovat soukromí zaměstnance jen v rozsahu, který je nezbytný k výkonu práce, případně k ochraně majetku zaměstnavatele.*"[62]

Zaměstnavatelem vybraný způsob a rozsah kontroly zaměstnanců tak v každém případě musí projít testem proporcionality. Dle Morávka se zákonným stane pouze takové monitorování, které představuje co nejmenší možný zásah do práv zaměstnanců a je vhodné k dosažení zamýšleného účelu. Dále nesmí být možné tohoto účelu dosáhnout za použití jiného, méně invazivního prostředku.[63] Poslední podmínku je obzvláště náročné splnit v případě instalace kamerových systémů, které Nejvyšší správní soud shledal za výjimečně invazivní prostředek

[60] V porovnání např. s rozhodnutími Úřadu pro ochranu osobních údajů, které jsou přístupné na webových stránkách Úřadu.
[61] MORÁVEK, J. § 316 [Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance]. In: PICHRT, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.
[62] Rozsudek Nejvyššího správního soudu ze dne 23. 08. 2013, sp. zn. 5 As 158/2012 - 49
[63] MORÁVEK, J. § 316 [Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance]. In: PICHRT, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.

kontroly.[64] Výše uvedený test proporcionality je v praxi běžně aplikován inspektoráty práce při kontrole kamerových systémů na pracovištích.[65]

Při hodnocení přiměřenosti sledování pomocí kamerového systému se musí vzít v potaz množství faktorů, např. počet kamer, umístění a namíření kamer (dle Hůrky musí být kamery „*směřován*[y] *na majetek zaměstnavatele, nikoliv na osobu zaměstnance*“),[66] dobu spuštění kamer (během či mimo pracovní dobu) či doba uchování záznamů.[67] Méně invazivním je např. sledování společných prostor a chodeb, větší zásah do soukromí pak představuje konstantní monitorování pracovních míst zaměstnanců. Kamery by pak v žádném případě neměly být umístěny či namířeny na soukromé prostory, jakými jsou např. sociální zařízení či sprchy.[68]

K danému tématu je vhodné zmínit i rozsudek Evropského soudu pro lidská práva ve věci *López Ribalda a ostatní proti Španělsku*[69], který stanovil kritéria, ke kterým je nutno přihlédnout při zkoumání přiměřenosti sledování zaměstnanců na pracovišti pomocí kamerových systémů:

„*(i) zda byl zaměstnanec o možnosti sledování kamerovým systémem v zásadě předem informován; (ii) jaký byl rozsah sledování a stupeň zásahu do soukromí zaměstnance, kdy se zkoumá časový a prostorový rozsah sledování a počet osob majících přístup k záznamům; (iii) zda měl zaměstnavatel pro monitorování legitimní důvody; (iv) zda zaměstnavatel mohl uplatnit méně invazivní zásah do soukromí než monitorování; (v) jaké byly výsledné dopady monitorování na zaměstnance; a (vi) zda měl zaměstnanec k dispozici adekvátní záruky, zejména zda zaměstnavatel mohl zaměstnance sledovat jen po výslovném předchozím upozornění.*“[70]

---

[64] Srov. rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013 sp. zn. 5 As 158/2012- 49: „*Nejvyšší správní soud považuje za nutné zdůraznit, že k instalaci kamerových systémů, s ohledem na jejich povahu a zásah do osobní integrity osob, je možné přistoupit až tehdy, pokud už veškeré méně invazivní prostředky selhaly anebo by nebyly schopny naplnit vytyčený účel, který je sledován. Je zcela nepochybné, že kamerový systém ve srovnání s jinými prostředky (např. personálními, mechanickými), které mohou dosáhnout naplnění účelů žadatelem sledovanými, zasahuje základní lidská práva, a to právo na soukromí a na soukromý rodinný život, která jsou garantována čl. 10 Listiny základních práv a svobod a v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod, a tudíž i do lidské důstojnosti, z které tato práva vyplývají.*“

[65] Viz Příkaz Oblastního inspektorátu práce pro Ústecký a Liberecký kraj pod sp. zn. S7-2020-171, Rozhodnutí Oblastního inspektorátu práce pro Jihomoravský a Zlínský kraj pod sp. zn. S9-2019-323 a Příkaz Oblastního inspektorátu práce pro Jihomoravský a Zlínský kraj pod sp. zn. S9-2020-373, které tvoří Přílohy č. 2-4 této diplomové práce

[66] Rozsudek Nejvyššího správního soudu ze dne 23. 08. 2013, sp. zn. 5 As 158/2012 - 49

[67] JANEČKOVÁ, E. a BARTÍK, V. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi).* Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3. S. 133.

[68] Úřad pro ochranu osobních údajů. *Stanovisko č. 1/2006 - Provozování kamerového systému z hlediska zákona o ochraně osobních údajů* [on-line]. 2006. Dostupné z: https://old.uoou.cz/files/stanovisko_2006_1.pdf

[69] Rozsudek Velkého senátu ESLP ze dne 17. října 2019 ve věcech č. 1874/13 a 8567/13 – López Ribalda a ostatní proti Španělsku

[70] V předmětném rozhodnutí ESLP odkazuje na své dřívější rozhodnutí ve věci *Bărbulescu proti Rumunsku,* které stanovilo kritéria pro hodnocení přiměřenosti monitorování komunikace zaměstnanců a konstatuje, že daná kritéria lze přiměřeně uplatnit i v případě sledování pomocí kamerových systémů, Viz § 102 rozhodnutí *Bărbulescu proti Rumunsku*: *„Vnitrostátní soudy proto v obdobných případech musí zkoumat: (i) zda byl zaměstnanec o možnosti*

2.2.3. Informační povinnost

Jak vyplývá i z výše vymezených kritérií ESLP, informování zaměstnance o možnosti a rozsahu sledování je důležitou podmínkou pro zmírnění zásahu do soukromí zaměstnanců a zachování tak přiměřenosti kontroly. Zákoník práce informační povinnost přímo zakotvuje ve svém § 316 odst. 3, dle kterého je zaměstnavatel provádějící kontrolu zaměstnanců v souladu s podmínkami § 316 odst. 2 ZPr „*povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění*". Obdobnou povinnost, která se uplatní v případě, že při kontrole dochází ke zpracování osobních údajů (tj. pokud snímané osoby lze identifikovat) nalezneme i v článcích 12 a násl. GDPR, tou se však tato práce bude zabývat až v následujících kapitolách.

Povinnost dle § 316 odst. 3 ZPr má hned několik rovin, které lze rozebrat. První je otázka formy, ve které má být informace zaměstnancům sdělena – zde zákoník práce stanoví pouze povinnost zaměstnance informovat „přímo". Dle Kottnauera je pod přímou informovaností nutno chápat „*že jeden každý zaměstnanec bude o prováděné kontrole a sledování vyrozuměn příslušným vedoucím zaměstnancem.*"[71] Morávek přímé informování zaměstnance vykládá mnohem šířeji, jako „*adresné předání informace zaměstnanci, tedy poskytování informace kanálem, s nímž se zaměstnanec seznámit musí, jako je řádně vyhlášený a přijatý vnitřní předpis, nebo kanálem, jímž zaměstnavatel zaměstnance sám přímo informuje (ústní sdělení, písemné sdělení, zpráva elektronické pošty).*" [72]

Za přiměřenější lze považovat širší výklad, také z toho důvodu, že by osobní informování každého zaměstnance jeho vedoucím zaměstnancem mohlo být nepraktické a z důvodu širokého obsahu poskytovaných informací i nepřesné. Mnohem vhodnějším se jeví sdělení prostřednictvím vnitřního předpisu, případně jiného písemného dokumentu. V případě kamerových systémů lze uvažovat i o instalaci informačních tabulí v prostorách, monitorovaných kamerami.[73] Úřad navrhuje předání informací ve dvou úrovních, a to umístěním dobře viditelných a čitelných

---

monitorování a jeho samotném výkonu předem informován; (ii) jaký byl rozsah monitorování a stupeň zásahu do soukromí zaměstnance, kdy je zásadní rozdíl mezi sledováním toku komunikace a jejího obsahu; (iii) zda měl zaměstnavatel legitimní důvody ospravedlňující monitorování probíhající komunikace a následné nahlédnutí do ní; (iv) zda zaměstnavatel mohl uplatnit méně invazivní zásah do soukromí než přímé nahlédnutí do komunikace zaměstnance; (v) jaké byly výsledné dopady monitorování na zaměstnance; a (vi) zda měl zaměstnanec k dispozici adekvátní záruky, zejména zda zaměstnavatel mohl sledovat obsah komunikace jen po výslovném předchozím upozornění zaměstnance."

[71] KOTTNAUER, A. § 316. In: KOTTNAUER, A. *Zákoník práce: komentář*. Praha: Leges, 2012. Komentátor. ISBN 978-80-87576-08-3.

[72] MORÁVEK, J. § 316 [Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance]. In: PICHRT, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.

[73] LANDWEHRMANN, T. *Zavedení kamerového systému na pracovišti (vzor směrnice).* Praktická personalistika č. 7-8/2021. ANAG. s. 35 – 42. ISSN:2336-5072

informačních tabulek v monitorovaných prostorech i poskytnutím podrobných informací každé dotčené osobě v textové podobě.[74]

Sdělované informace mají dle zákoníku práce obsahovat údaj o „rozsahu“ a „způsobu provádění“ kontroly. Dle Morávka je „rozsahem“ myšleno „*označení pracovních povinností, které budou kontrolovány, včetně např. činností, které budou kontrolovány, a období, kdy bude kontrola probíhat, příp. včetně sledovaných prostor*“.[75] V případě kontroly kamerovým systémem si pod „rozsahem“ kontroly lze představit i počet a umístění nainstalovaných kamer, monitorované prostory či úhel namíření kamer a dobu, kdy budou kamery snímat. Za informování o „způsobu provádění“ kontroly pak Morávek považuje uvedení druhu kontrolního mechanismu.[76]

Informační povinnost lze zkoumat i z časového hlediska. Zákoník práce sice přímo nestanoví, že by k informování zaměstnance mělo docházet už před započetím kontroly, ale tuto povinnost lze dovodit z judikatury. Nejvyšší správní soud ve svém rozsudku se sp. zn. 5 As 158/2012 – 49 uvádí, že „*monitoring zaměstnance je možný pouze na základě předchozího oznámení*“, s tím že „*předmětem informace zaměstnanci před započetím monitoringu je rovněž rozsah a způsob provádění kontroly.*“

2.2.4. Skryté sledování

V návaznosti na judikaturou stanovenou povinnost informovat zaměstnance o monitorování ještě před jeho započetím se nabízí další otázka, a to jak může zaměstnavatel postupovat, pokud chce zavést skryté sledování. Dle Morávka musí zaměstnavatel v takovém případě splnit informační povinnost až po jejím skončení, avšak „*v obecné rovině musí zaměstnavatel možnou kontrolu deklarovat alespoň rámcově předem.*“[77] Ministerstvo vnitra ČR ve svém stanovisku však zaujímá kategoričtější postoj a uvádí, že s ohledem na informační povinnost dle § 316 odst. 3 ZPr „*skryté sledování zaměstnanců v tomto případě nepřipadá v úvahu*“.[78] Lze tedy polemizovat, zda je skryté sledování dle právního řádu vůbec možné.

---

[74] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 10.
[75] MORÁVEK, J. § 316 [Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance]. In: PICHRT, J. *Zákoník práce: Zákon o kolektivním vyjednávání*. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.
[76] Tamtéž.
[77] Tamtéž.
[78] Ministerstvo vnitra České republiky. *Stanovisko ke kontrole výkonu pracovní činnosti strážníků prostřednictvím GPS lokátorů umístěných ve vozidlech a radiostanicích obecní policie*. [on-line]. 2021. Dostupné z: https://www.mvcr.cz/soubor/stanovisko-ke-kontrole-vykonu-pracovni-cinnosti-strazniku-prostrednictvim-gps-lokatoru-umistenych-ve-vozidlech-a-radiostanicich-obecni-policie.aspx

Skryté sledování představuje nepochybně významnější zásah do soukromí než sledování otevřené, dle Štefka dokonce nepřípustný: „*Použití skrytého sledování ke kontrole určité skupiny osob totiž zpravidla představuje nepřípustný zásah do soukromí těchto osob, takové jednání je možné pouze na základě zákona a v jeho mezích (např. v trestním řízení).*“[79]

Otázkou přiměřenosti takového zásahu do soukromí se zabýval ESLP. Ve věci *López Ribalda a ostatní proti Španělsku* neoznačil skryté sledování kamerovým systémem, o kterém zaměstnanci nebyli předem vůbec informováni, za porušení práva na soukromí dle čl. 8 Úmluvy o ochraně lidských práv a základních svobod.[80] I když tato absence upozornění byla v rozporu s vnitrostátním právem i s jedním z kritérií přiměřenosti kamerového sledování, vymezených ESLP ve stejném rozsudku[81], ESLP shledal, že se jedná „*pouze o jedno z kritérií vzatých v úvahu při posuzování přiměřenosti přijatého opatření*“ a že při nenaplnění tohoto kritéria pouze bude přísněji vymáhat splnění ostatních. Jelikož zaměstnavatel ve zkoumaném případě měl pádný důvod k instalaci skrytého kamerového systému a skryté sledování bylo prováděno pouze v nutném rozsahu,[82] ESLP rozhodl, že jím prováděné monitorování nepředstavovalo nepřiměřený zásah do práva na soukromí zaměstnanců.[83] Potvrdil tak i své předchozí rozhodnutí ve věci *Köpke proti Německu*, ve kterém také označil skryté sledování zaměstnankyně z důvodu podezření na krádež za přiměřené.[84]

V české judikatuře také můžeme najít rozhodnutí, ve kterém bylo skryté sledování zaměstnance označeno jako zákonné, a to rozsudek Nejvyššího soudu se sp. zn. 21 Cdo 1771/2011. V projednávané věci se jednalo o skryté sledování internetových aktivit zaměstnance.[85] Nejvyšší soud shledal, že se v tomto případě nejednalo o skryté sledování ve smyslu § 316 odst. 2 ZPr, ale pouze o kontrolu využití výrobních a pracovních prostředků ve smyslu § 316 odst. 1. Argumentoval cílem kontroly, jímž dle Nejvyššího soudu nebylo „*zjišťování obsahu e-mailových zpráv, obsahu SMS nebo MMS, případně odeslaných či přijatých zaměstnancem*“, pouze „*zjištění, zda zaměstnanec (žalobce) respektuje (a když nerespektuje, tak v jaké míře) zákaz užívat pro svou osobní potřebu výpočetní techniku zaměstnavatele (žalovaného) včetně jeho telekomunikačních*

---

[79] ŠTEFKO, M. *K problému sledování vlastních zaměstnanců*. Právo a zaměstnání č. 1/2005. LexisNexis CZ. S. 7-11. Dostupné z: https://www.sagit.cz/info/k-problemu-sledovani-vlastnich-zamestnancu#kamerov%C3%A9

[80] Srov. znění článku 8 ÚLPZS: „Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.“

[81] „*(i) zda byl zaměstnanec o možnosti sledování kamerovým systémem v zásadě předem informován“*

[82] Zaměstnavatel měl podezření, že v monitorované prodejně dochází ke krádežím (z důvodu ztrát v tržbách) Skryté kamery pak byly namířeny pouze na pokladny, tj. na místo, kde ke krádeži mohlo docházet.

[83] Rozsudek ESLP ze dne 17. října 2019 ve věcech č. 1874/13 a 8567/13 – López Ribalda a ostatní proti Španělsku

[84] Srov. rozsudek ESLP ze dne 5. října 2010 ve věci 420/07 – Köpke proti Německu

[85] V tomto případě zaměstnavatel monitoroval, jaké internetové stránky zaměstnanec navštěvoval v pracovní době na pracovním přístroji.

zařízení“ a mírou zásahu do soukromí zaměstnance, kterou Nejvyšší soud označil za „*zcela zanedbatelnou*“.[86] V tomto případě tak nebylo nutno plnit informační povinnost dle § 316 odst. 3 ZPr, jelikož ta je navázána na kontrolu zaměstnanců dle § 316 odst. 2 ZPr.

Skryté sledování zaměstnanců výhradně za účelem kontroly zákazu dle § 316 odst. 1 ZPr se tedy zdá jako možné. Výše uvedený judikát se však nevěnoval přímo kamerovým systémům a je tak otázkou, zda by skryté sledování tak invazivním kontrolním prostředkem mohlo spadat pouze pod § 316 odst. 1 ZPr. ESLP sice v rozhodnutí *López Ribalda a ostatní proti Španělsku* označil skryté sledování pomocí kamerového systému za přiměřený zásah do soukromí, nepochybně však o zásah do soukromí šlo, a to nikoli „zcela zanedbatelný“. Lze se domnívat, že sledování zaměstnanců kamerovým systémem by s sebou vždy neslo nezanedbatelnou úroveň narušení soukromí, a tak by vždy spadalo pod úpravu § 316 odst. 2 a 3 ZPr.

Judikaturou ještě nebyla řešena otázka skrytého sledování zaměstnanců dle § 316 odst. 2 ZPr a možnost případného splnění informační povinnosti dle § 316 odst. 3 ZPr až po skončení takového sledování. Při absenci jakýchkoli vodítek či stanovisek k této problematice se lze přiklonit spíše k názoru, že informační povinnost dle § 316 odst. 3 ZPr je nutno v souladu s judikaturou Nejvyššího správního soudu[87] splnit vždy před započetím jakéhokoli sledování, a to v plném rozsahu. Skryté sledování zaměstnanců kamerovým systémem tak lze dle současné právní úpravy a judikatury považovat za principiálně nezákonné.

Lze ale také polemizovat, zda se nejedná o příliš restriktivní výklad, který neúměrně omezuje zájmy zaměstnavatele. Jako možnost se nabízí poskytnutí informací dle § 316 odst. 3 ZPr před započetím sledování pouze v obecné rovině. V praxi by se jednalo o informování zaměstnanců, že ke sledování určených oblastí pracoviště pomocí kamerového systému může či nemusí v blízké době dojít. Tímto by mohla být splněna informační povinnost a zaměstnavatel by si ponechal možnost „částečně skrytého“ sledování, které by mohlo vést k efektivnějšímu odhalení případného protiprávního jednání.

V současnosti se však nedá s jistotou říci, který z výše uvedených výkladů problematiky skrytého sledování zaměstnanců je vhodnější. Lze pouze doufat, že v blízké době dojde k potvrzení jednoho z výkladů Úřadem či v judikatuře, případně k aktualizaci právní úpravy obsažené v § 316 ZPr.

[86] Rozsudek Nejvyššího soudu ze dne 16. 08. 2012, sp. zn. 21 Cdo 1771/2011
[87] Rozsudek Nejvyššího správního soudu ze dne 23. 08. 2013, sp. zn. 5 As 158/2012 – 49

3. Atrapy kamer na pracovišti

Při použití atrap kamer nedochází ke zpracování osobních údajů, a tak se na ně nevztahuje obecné nařízení, jak vyplývá i z příkladu k bodu 8 Pokynů 3/2019, ve kterém Sbor stanoví, že „*Nařízení GDPR se nevztahuje na falešné kamery (tj. jakékoli kamery, které nefungují jako kamery, a proto nezpracovávají žádné osobní údaje).*“[88] Dále se na atrapy kamer neaplikují ani povinnosti, vyplývající z § 316 ZPr, jelikož se jejich prostřednictvím nekoná monitorování zaměstnanců.

Nelze však dojít k závěru, že užití atrap kamer nepodléhá žádné regulaci a nemůže představovat zásah do práv a svobod osob i přesto, že využití atrap kamer bývá Úřadem doporučováno jako alternativa k instalaci kamerového systému.[89] Z rozhodovací praxe inspektorátu práce vyplývá, že nepřiměřené umisťování atrap kamer na pracovišti může být v rozporu se zákoníkem práce.

3.1. Rozhodovací praxe inspektorátu práce

V případě nejmenované dopravní společnosti bylo inspektorátem práce v instalaci atrap kamer shledáno porušení ustanovení zákoníku práce, konkrétně povinnosti vytvářet příznivé pracovní podmínky dle § 302 písm. c) ZPr.

Podnět k prošetření tohoto případu nejprve směřoval na Úřad pro ochranu osobních údajů. Podle stížnosti zaměstnanců měl jejich zaměstnavatel „*neoprávněně monitorovat a pořizovat záznamy z prostoru sociálního zařízení sloužícího pro zaměstnance.*“[90] Úřad na základě této stížnosti provedl šetření na předmětném pracovišti. Během kontroly vyšlo najevo, že se však jedná pouze o atrapu kamery, neschopnou zpracování osobních údajů.[91] Úřad tak nemohl proti společnosti zahájit správní řízení. Ve svém protokolu ke kontrole[92] však posoudil instalaci atrap

[88] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 7-8.
[89] Srov. Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 9.
[90] Úřad pro ochranu osobních údajů. *Přepravní a dopravní společnost – Kontrola kamerového systému se zaměřením na zaměstnance společnosti (UOOU-04151/20)* [on-line]. 2021. Dostupné z: https://old.uoou.cz/prepravni-a-dopravni-spolecnost-kontrola-kameroveho-systemu-se-zamerenim-na-zamestnance-spolecnosti-uoou-04151-20/ds-7043/archiv=0&p1=5209
[91] Tamtéž.
[92] Úřad pro ochranu osobních údajů. *Anonymizovaný protokol o kontrole (UOOU-04151/20-16)* [on-line]. 2021. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=55777

na sociálním zařízení „*jako nátlakově nepatřičné jednání vůči zaměstnancům a dalším osobám, a zasahující do jejich osobnostních práv*“ a postoupil případ místnímu inspektorátu práce.

Výsledky následné kontroly inspektorátem práce lze dovodit z tiskové zprávy[93] Úřadu ze dne 10. května 2022, ve které Úřad uvedl, že „*Inspektorát práce pochybení potvrdil a konstatoval, že zaměstnavatel instalací atrapy technologických prvků kamerového systému porušil zákoník práce (§ 302, písm. c) zák. č. 262/2006 Sb., konkrétně povinnost „vytvářet příznivé pracovní podmínky a zajišťovat bezpečnost a ochranu zdraví při práci“).*“ [94] Je nutno podotknout, že se zatím jedná o jediné známé rozhodnutí inspektorátu práce, které by se této problematice věnovalo.

Příznivé pracovní podmínky

Lze diskutovat, zda odkaz na ustanovení § 302 ZPr je v tomto případě vhodný. Zmíněné ustanovení totiž stanovuje povinnosti nikoli přímo zaměstnavateli, nýbrž vedoucím zaměstnancům.[95] Odkaz na toto ustanovení je nicméně možné považovat za výkladové překlenutí mezery v zákoníku práce. Právo zaměstnanců na „uspokojivé pracovní podmínky“ zakotvuje již čl. 28 Listiny základních práv a svobod, v zákoníku práce pak na něj pamatuje § 1a odst. 1 písm. b), který vyjadřuje základní zásady pracovněprávních vztahů. Zákoník práce však nikde explicitně nestanoví zaměstnavateli povinnost uspokojivé či příznivé podmínky vytvářet a udržovat.[96]

Následně je nutno se vypořádat s otázkou, zda umisťování nefunkčních kamer na sociální zařízení zaměstnanců opravdu vytváří nepříznivé pracovní podmínky. Lze tvrdit, že ano, jelikož i pouhé vytvoření dojmu sledování zaměstnance v tak soukromých prostorách bude pro zaměstnance minimálně velice nepříjemné. K tomuto lze citovat z jiného rozhodnutí inspektorátu práce: „*V případě, že je zaměstnanec monitorován i v prostorách určených k odpočinku, je to pro něj velmi nepříjemné, neboť je sledován v době, kdy má právo na svoje soukromí. Sledování zaměstnance prostřednictvím kamerového systému v době odpočinku může ovlivňovat jeho psychický stav a sebeúctu a může rovněž zhoršovat pracovní výkonnost zaměstnance. Lze tak*

[93] Dané rozhodnutí inspektorátu práce se autorce práce bohužel nepodařilo získat ani na základě žádosti dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Kontext předmětného rozhodnutí se tak může lišit v závislosti na konkrétních skutkových zjištěních.

[94] Úřad pro ochranu osobních údajů. *Kamerová atrapa sice GDPR neporušuje, ale její instalace může být sankcionována* [on-line]. 2022. Dostupné z: https://old.uoou.cz/kamerova-atrapa-sice-gdpr-neporusuje-ale-jeji-instalace-muze-byt-sankcionovana/d-55810

[95] § 302 ZPr zní: „*Vedoucí zaměstnanci jsou dále povinni…*
…c) vytvářet příznivé pracovní podmínky a zajišťovat bezpečnost a ochranu zdraví při práci“

[96] Srov. § 224 odst. 1 ZPr, který zakotvuje pouze povinnost zaměstnavatele „*vytvářet zaměstnancům pracovní podmínky, které umožňují bezpečný výkon práce*“.

konstatovat, že ze strany zaměstnavatele se jedná o opatření vedoucí k vytváření zneklidňujícího prostředí na pracovišti, což může vést i k narušení vztahů na pracovišti."[97]

3.2. Domnělé sledování a právo na ochranu soukromí zaměstnance

Stojí za zvážení, zda obdobné domnělé sledování pomocí atrap kamer nemůže představit i zásah do soukromí zaměstnance. Málek a Veselý se domnívají, že ano, dle jejich názoru k zásahu do soukromí „*dochází, aniž by byl fakticky pořízen záznam*".[98] Lze souhlasit s tímto posouzením, jelikož dotčený zaměstnanec bude při domnělém sledování zásah do soukromí vnímat bez ohledu na to, zda ke sledování reálně dochází.

Tato situace je také ztížena skutečností, že se na atrapy kamer neaplikuje informační povinnost vyplývající z § 316 odst. 3 ZPr. Dotčený zaměstnanec tak nemá možnost rozpoznat, že se jedná pouze o napodobeninu kamerového systému a právem tak může považovat jejich užití za nezákonné.[99] Při aplikaci informační povinnosti i na atrapy kamer by ale tato zařízení pozbyla svého smyslu.[100] Lze tak konstatovat, že instalace atrap kamer na pracovišti je problematickou a málo diskutovanou oblastí, které by měla být věnována větší pozornost v odborné literatuře a právní úpravě.

---

[97] Viz Příkaz Oblastního inspektorátu práce pro hlavní město Prahu pod sp. zn. S3-2020-49, který tvoří Přílohu č. 1 této diplomové práce

[98] MÁLEK, Jakub a VESELÝ, Jakub. *Kamerové systémy na pracovišti a příznivé pracovní podmínky* [on-line]. 2022. pravniprostor.cz Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/kamerove-systemy-na-pracovisti-priznive-pracovni-podminky

[99] Jelikož z pohledu zaměstnance zaměstnavatel neplní své povinnosti vyplývající z § 316 ZPr.

[100] Po informování zaměstnanců o faktické nefunkčnosti kamerového systému nemůže tento systém plnit svou „odstrašující" funkci.

4. Podmínky užití kamerových systémů na pracovišti dle GDPR

Jak již bylo uvedeno v první kapitole této diplomové práce, užití kamerových systémů ve většině případů[101] představuje zpracování osobních údajů ve smyslu čl. 4 odst. 2 GDPR. Z GDPR pak vyplývá řada dalších povinností, které musí zaměstnavatel při instalaci kamerového systému na pracoviště splnit i nad rámec § 316 ZPr.

4.1. Působnost GPDR a výklad klíčových pojmů

Obecné nařízení o ochraně osobních údajů neboli GDPR je přímo použitelným právním předpisem Evropské unie, věnujícím se ochraně osobních údajů a právu na soukromí fyzických osob na území EU. V květnu roku 2018 nahradilo předchozí právní úpravu ve formě směrnice 95/46/ES[102] a její odraz v českém právním řádu, zákon o ochraně osobních údajů.

Dle čl. 2 odst. 1 GDPR se nařízení „*vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny*“. K tomu, aby bylo toto vymezení plně srozumitelné, je nutno si nejdříve definovat pojmy „zpracování osobních údajů“ a „osobní údaj“.

Pojem „osobní údaj“

Za „osobní údaj“ označuje GDPR ve svém čl. 4 odst. 1 „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby*“. Z hlediska této definice je rozhodující možnost identifikace konkrétní fyzické osoby pomocí osobního údaje či jejich souboru.[103]

Za osobní údaj dle GDPR je třeba považovat i fotografii či videozáznam osoby, pokud na takovém médiu bude rozeznatelná. Dle Úřadu je fyzická osoba, snímaná kamerovým systémem „*identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické*

[101] O zpracování osobních údajů se nejedná např., pokud nízké rozlišení kamer neumožňuje identifikovat jednotlivé fyzické osoby v záběru.
[102] 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
[103] Typicky by se jednalo o jednoznačný identifikátor, jako je např. rodné číslo, či o kombinaci osobních údajů, pomocí které lze bezpečně identifikovat konkrétní osobu, jako je jméno společně s místem bydliště a datem narození osoby.

rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby.“[104] Evropský sbor pro ochranu osobních údajů pak v bodě 7 *Pokynů 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* uvádí, že monitorování určitého prostoru mj. audiovizuálními prostředky „*vede ke shromažďování a uchovávání obrazových nebo audiovizuálních informací o všech osobách vstupujících do monitorovaného prostoru, které lze identifikovat na základě jejich vzhledu nebo jiných charakteristických znaků. Na základě těchto údajů lze zjistit totožnost těchto osob.*“

Dle Jarolímkové se pak za osobní údaje považují i přenosy videa, snímané on-line kamerovými systémy bez záznamu: „*ve většině případů bude nutné za osobní údaj na rozdíl od původní praxe ÚOOÚ považovat i pouhý přenos videa, například webovou kamerou, bez ukládání záznamu, resp. jen s technicky nezbytnou úrovní ukládání pro přenos*.“[105]

Zvláštní kategorie osobních údajů

Pro úplnost je nutno zmínit, že GDPR dále ve svém čl. 9 vymezuje zvláštní kategorii osobních údajů, se kterou spojuje vyšší právní ochranu.[106] Do ní řadí údaje „*které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby*“. Z fotografií či videozáznamů osob lze zpravidla rozpoznat jejich rasový původ a obě média mohou sloužit i jako biometrický údaj.[107] Lze si tak položit otázku, zda veškeré fotografie a videozáznamy osob spadají do zvláštní kategorie osobních údajů.

Tímto problémem se zabýval ve svém *Stanovisku č. 12/2012 K použití fotografie, obrazového a zvukového záznamu fyzické osoby* Úřad pro ochranu osobních údajů. Dle Úřadu záleží na účelu zpracování informací získaných z fotografie anebo videozáznámu: „*Jestliže jsou však informace z fotografie subjektu údajů používány pro pouhé rozlišení jeho podoby ve srovnání*

---

[104] Úřad pro ochranu osobních údajů. *K provozování kamer a kamerových systémů* [on-line]. 2022. Dostupné z: https://old.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=29535&n=k%2Dprovozovani%2Dkamer%2Da%2Dkamerovych%2Dsystemu&p1=1099

[105] JAROLÍMKOVÁ, A. Článek 4. [IV. Fotografie a videozáznam jako osobní údaj]. In: UŘIČAŘ, M. *Obecné nařízení o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.

[106] K zákonnému zpracování zvláštních osobních údajů je nutno splnit přísnější podmínky, srov. čl. 9 GDPR

[107] „Biometrickými údaji“ se dle čl. 4 odst. 14 GDPR rozumí „*osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje*“

s jinými osobami a tyto informace nejsou dále zpracovávány, nelze takové používání fotografií posuzovat jako zpracování citlivých osobních údajů.“[108]

Na účel zpracování poukazuje i Morávek, který uvádí, že „*za rozhodující faktor tak lze (v tomto případě označit zejména účel, určené prostředky a způsob zpracování. Jejich souvztažnost bude určující pro to, zda pro daný případ bude nosič údajů prostředkem k pořízení citlivého údaje – zejména jedná-li se o údaj biometrický.*“ Zároveň upozorňuje na část recitálu č. 51 GDPR, která zní: „*Zpracování fotografií by 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 umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby*.“ [109]

Z výše uvedeného se dá usoudit, že se v obecné rovině fotografie či videozáznam nepatří do zvláštní kategorie osobních údajů. Jiná situace však nastane v případě pořízení či zpracování těchto médií přímo za účelem zisku biometrických údajů či jiných zvláštních osobních údajů.

Pojem „zpracování osobních údajů“

Dle čl. 4 odst. 2 GDPR je za „zpracování“ v tomto kontextu nutno považovat „*jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení*“.

Jelikož je fotografie či videozáznam rozpoznatelné fyzické osoby osobním údajem dle čl. 4 odst. 1 GDPR, je nepochybné, že je nahrávání zaměstnanců pomocí kamerového systému se záznamem ve většině případů zpracováním, jakožto shromažďování či zaznamenávání takových údajů. Zde je potřeba klást důraz na identifikovatelnost osob na záznamu – jak uvádí Sbor v bodě 8 Pokynů 3/201: „[n]*ařízení se však nevztahuje na zpracování údajů, které neodkazují na osobu, např. pokud jednotlivec nemůže být přímo nebo nepřímo identifikován.*“. Dle Pokynů 3/2019 např. záznamy z vysokých výšek jsou zpracováním dle GDPR „*pouze tehdy, pokud zpracované údaje*

[108] Úřad pro ochranu osobních údajů. *Stanovisko č. 12/2012 - K použití fotografie, obrazového a zvukového záznamu fyzické osoby* [on-line]. 2012. Dostupné z: https://old.uoou.cz/files/stanovisko_2012_12.pdf
[109] MORÁVEK, J. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer, 2019. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-587-3. S. 129-130.

mohou být za určitých okolností spojeny s konkrétní osobou.“[110]

Podle Morávka je označení pořizování záznamu kamerovým systémem za zpracování „*podmíněn*[o] *alespoň minimální a reálnou pravděpodobností zachycení fyzické osoby (anebo skutkového děje podávajícího informace mající povahu osobních údajů v zorném poli kamery, stejně jako technickou způsobilost zařízení zachytit dostatečné množství konkrétních znaků, na základě kterých může být příslušný subjekt údajů určený, anebo určitelný.*“[111] Toto vymezení konkretizuje Úřad v čl. 2.2 Návrhu metodiky určením, že identifikovatelné[112] mohou být osoby pouze na záběrech kamerových systémů s rozlišením více než 40 mm na pixel.[113]

K otázce, zda za zpracování ve smyslu GDPR lze považovat i on-line monitorování kamerovým systémem bez možnosti záznamu, je nutno opět poukázat na stanovisko *K provozování kamer* Úřadu pro ochranu osobních údajů, ve kterém uvádí, že „*provozování kamerového systému je považováno za zpracování osobních údajů podléhající povinnostem podle obecného nařízení, pokud je automatizovaně prováděn záznam monitorovaného veřejného prostoru, nebo dochází k šíření obrazového nebo audiovizuálního signálu monitorovaného veřejného prostoru obsahujícího údaje využitelné k identifikaci fyzických osob,*[…]“[114] a čl. 2.3 Návrhu metodiky, v němž Úřad považuje za zpracování osobních údajů také „*Prohlížení on-line záběrů z kamerového systému (snímaní, přenos, zobrazení).*“[115]

Výjimky z věcné působnosti GDPR

Nyní je možné se vrátit zpět ke znění čl. 2 odst. 1 GDPR.[116] Z tohoto ustanovení *a contrario* vyplývá, že se nařízení nevztahuje na neautomatizované zpracování osobních údajů, které nejsou anebo nemají být zařazeny v evidenci.[117]

---

[110] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 7.
[111] Tamtéž. S. 132.
[112] Bez použití nadměrného úsilí.
[113] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 4.
[114] Úřad pro ochranu osobních údajů. *K provozování kamer a kamerových systémů* [on-line]. 2022. Dostupné z: https://old.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=29535&n=k%2Dprovozovani%2Dkamer%2Da%2Dkamerovych%2Dsystemu&p1=1099
[115] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 5.
[116] Čl. 2 odst. 1 GDPR zní: „*Toto nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny*“.
[117] Za „evidenci“ se dle čl. 4 odst. 6 GDPR považuje „*jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska*“.

V případě sledování kamerovým systémem se nepochybně bude jednat o automatizované zpracování.[118] Pro tento proces tak není zásadní, zda budou takto získané osobní údaje zařazovány do evidence.

Dle čl. 2 odst. 2 písm. c) se GDPR dále nevztahuje na jakékoli zpracování, prováděné „*fyzickou osobou v průběhu výlučně osobních či domácích činností*". Ze znění této výjimky lze dovodit, že se zajisté nevztahuje na jakékoli zpracování prováděné zaměstnavatelem na pracovišti, tj. ani na sledování zaměstnanců kamerovým systémem. Toto potvrzuje i recitál GDPR č. 18, který uvádí, že se GDPR nevztahuje na činnosti, prováděné „*bez jakékoliv souvislosti s profesní nebo obchodní činností*."

Instalace a provoz kamerového systému na pracovišti tak dle výše uvedeného spadá pod věcnou působnost GDPR, a to i v případě on-line monitorování bez záznamu. Výjimkou je provozování kamer, na jejichž záběrech by nebylo možné identifikovat žádnou fyzickou osobu.[119]

4.2. Právní základ ke zpracování osobních údajů

Zpracování osobních údajů je dle GDPR zákonné pouze tehdy, pokud k němu má správce[120] právní titul. Zpracování prováděné bez platného právního titulu je již od počátku nelegální. Správce tak musí tuto otázku zkoumat již před započetím zpracování – zda k zamýšlenému účelu zpracování existuje vhodný právní základ a zda rozsah a způsob zpracování odpovídá podmínkám vybraného právního základu, typicky zda je splněna podmínka nezbytnosti.

Možné právní tituly jsou taxativně[121] vyjmenovány v čl. 6 odst. 1 GDPR:

„*Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:*

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

---

[118] Viz např. bod 25 rozsudku Soudního dvora EU ve věci C-212/13

[119] Např. kamery, namířené pouze na vnitřek trezoru nebo kamery v tak vysoké výšce či s tak nízkým rozlišením, že ze záběrů nelze rozpoznat jednotlivé osoby.

[120] „Správcem" je dle čl. 4 odst. 7 GDPR „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení*". V kontextu této práce je správcem typicky zaměstnavatel.

[121] Srov. bod 49 rozsudku Soudního dvora EU ze dne 24. listopadu 2011 ve věcech Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) a Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10).

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.“

Z těchto možných právních základů zpracování jsou pro účely této práce nejrelevantnější právní tituly uvedené v písm. a) a f) výše uvedeného ustanovení, tedy souhlas subjektu údajů a oprávněný zájmu správce. Zbylé právní tituly se ve zkoumané problematice kamerových systémů na pracovišti uplatní spíše okrajově.

4.2.1. Souhlas subjektu údajů

V předchozí právní úpravě[122] měl souhlas subjektu údajů oproti ostatním právním titulům zvláštní postavení. Správce mohl zpracovávat osobní údaje primárně se souhlasem subjektu údajů. Ostatní právní tituly pak byly dle Úřadu pro ochranu osobních údajů považovány spíše za výjimky, které bylo nutno vykládat co nejúžeji.[123] Souhlas byl tak považován za jakýsi “základní” či “nejvhodnější” právní titul.[124] V GDPR však toto rozdělení již nenajdeme, souhlas je pouze jedním z šesti možných právních důvodů zpracování. V případě zpracování pomocí kamerového systému Úřad právní titul souhlasu dokonce nedoporučuje.[125]

I tak může řada zaměstnavatelů při zpracování osobních údajů v rámci pracovněprávních vztahů sáhnout ze všeho nejdříve po souhlasu, také proto, že se ze všech právních titulů zpracování

[122] V zákoně č. 101/2000 Sb., o ochraně osobních údajů, který se vstupem v platnost GDPR byl zrušen k 24. 04. 2019.
[123] Úřad pro ochranu osobních údajů. *Desatero omylů*. [on-line]. Dostupné z: https://old.uoou.cz/desatero-omylu/ds-4818/archiv=0
[124] BREJCHOVÁ, D. Článek 6 [Zákonnost zpracování]. In: UŘIČAŘ, M. *Obecné nařízení o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.
[125] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 6.

dle GDPR jeví jako ten nejpřímočařejší. Je však udělení souhlasu zaměstnancem platným právním základem ke zpracování osobních údajů?

Platný souhlas musí být dle čl. 7 GDPR doložitelný, odlišitelný, srozumitelný a snadno přístupný, dle výkladových pokynů WP259[126] dále také svobodný, konkrétní, informovaný a jednoznačný. Podmínce svobodnosti se věnuje i recitál č. 43 GDPR, který stanoví, že "*vyjádření souhlasu nemělo představovat platný právní důvod pro zpracování osobních údajů ve zvláštním případě, kdy mezi subjektem údajů a správcem existuje jasná nerovnováha*". Recitál zmiňuje jako příklad zpracování orgánem veřejné moci, jasnou nerovnováhu mezi správcem a subjektem údajů můžeme však vypozorovat v podobě hospodářské závislosti i v pracovněprávních vztazích.

Dle stanoviska WP249[127] vzhledem k závislému vztahu mezi zaměstnavatelem a zaměstnancem „*zaměstnanci téměř nikdy nejsou schopni svobodně udělit, odmítnout nebo zrušit souhlas.*" Platný souhlas by bylo možno poskytnout pouze „*za výjimečných okolností, kdy se s přijetím nebo odmítnutím nabídky nepojí žádné důsledky*." Tento právní názor sdílí i nástupce pracovní skupiny W29, Evropský sbor pro ochranu osobních údajů a v bodu 47 Pokynů 3/2019 uvádí, že „*vzhledem k nerovnováze mezi zaměstnavateli a zaměstnanci by se zaměstnavatelé ve většině případů neměli při zpracování osobních údajů opírat o souhlas, protože je nepravděpodobné, že bude dán svobodně*."[128]

Souhlas zaměstnance tedy není v pracovněprávních vztazích vhodným titulem ke zpracování. Zaměstnavatel jakožto správce musí zvolit jiný právní základ, kterým je v případě kamerových systémů na pracovišti typicky oprávněný zájem dle čl. 6 odst. 1 písm. f) GDPR.

4.2.2. Oprávněný zájem zaměstnavatele

Jak již vyplývá z výše uvedeného znění čl. 6 odst. 1 písm. f) GDPR, k užití právního titulu oprávněného zájmu nestačí pouhá existence takového zájmu, kterým může být např. zájem na ochraně majetku. Platnost a zákonnost tohoto právního titulu ke zpracování je nutno vždy posoudit

[126] Pracovní skupina zřízená podle článku 29. *Pokyny k souhlasu podle nařízení 2016/679* [on-line]. 2018. Dostupné z: https://ec.europa.eu/newsroom/article29/items/623051/en

[127] Pracovní skupina zřízená podle článku 29. *Stanovisko 2/2017 ke zpracování údajů na pracovišti* [on-line]. 2017. Dostupné z: https://ec.europa.eu/newsroom/article29/items/610169/en

[128] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 14.

dle tří kritérií, a to, zda oprávněný zájem správce vůbec existuje, zda je zpracování nezbytné, a nakonec zda nad zájmem správce nepřevažují zájmy subjektů údajů.[129]

Existence oprávněného zájmu

Dle recitálu č. 47 GDPR je oprávněný zájem dán např. v situaci, když „*existuje relevantní a odpovídající vztah mezi subjektem údajů a správcem, například pokud je subjekt údajů zákazníkem správce nebo mu naopak poskytuje služby*“. Podle stanoviska WP217[130] pak k tomu, aby byl zájem „oprávněný“, musí být zákonný, dostatečně konkrétní, skutečný a trvající (tj. nikoli spekulativní). Dle demonstrativního výčtu ve výše uvedeném stanovisku by existence oprávněného zájmu mohla být založena např. při sledování zaměstnanců pro účely bezpečnosti nebo řízení.

Dle Pokynů 3/2019 v případě dohledu kamerovým systémem k existenci oprávněného zájmu „*musí existovat argument reálného ohrožení – jako třeba škody nebo vážné incidenty v minulosti*.“ V Pokynech 3/2019 je dále doporučeno zdokumentovat veškeré důkazy existence hrozby (např. předchozí incidenty) a pravidelně přehodnocovat existenci oprávněného zájmu v konkrétních případech.[131] S tímto posouzením souzní i Úřad v čl. 3.1.1 Návrhu metodiky.[132]

V obecné rovině tak lze shledat, že např. zájem zaměstnavatele na ochraně majetku či zdraví zaměstnanců zakládá existenci oprávněného zájmu pro účely zpracování kamerovým systémem. Toto je však třeba posoudit u každé jednotlivé kamery s ohledem mj. na její umístění, zorné pole a dobu snímání.

Nezbytnost zpracování

Při posuzování kritéria nezbytnosti musí správce určit, zda je jím vybraný způsob a rozsah zpracování opravdu nutný k zajištění jeho oprávněného zájmu. Před zavedením kamerového dohledu za účelem ochrany majetku je tak nutno nejprve uvážit, jestli by zamýšleného účelu nešlo

---

[129] Tamtéž. S. 9.
[130] Pracovní skupina zřízená podle článku 29. *Stanovisko č. 6 /2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES* [on-line]. 2014. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf
[131] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 10.
[132] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 5.

dosáhnout i jinými prostředky – např. instalací bezpečnostních zámků či zavedením kontroly pomocí pracovníků.

Pokud se rozhodne pro kamerový systém, musí dále mj. posoudit, ve kterých prostorech a v jakou dobu je dohled pomocí kamer naprosto nezbytný. Důležité je i určení doby, po kterou budou záznamy z kamer ukládány (a jestli vůbec). Dle Pokynů 3/2019 se správce musí rozhodnout opět podle okolností jednotlivého případu: „*V některých případech může být nezbytné použít řešení černé skříňky, kde jsou záznamy po určité době uložení automaticky vymazány a přístup k nim je možný pouze v případě incidentu. V jiných situacích nemusí být nezbytné nahrávat jakýkoli videomateriál, ale vhodnější je namísto toho použít monitorování v reálném čase*."[133]

Poměřování zájmů

I při splnění výše uvedených kritérií je v každém konkrétním případě stále nutno posoudit, zda nad oprávněným zájmem správce nepřevažují zájmy či základní práva a svobody subjektů údajů. Takové posouzení lze vypracovat ve formě tzv. balančního testu. Balanční test je třeba provést v každém konkrétním případě zpracování, jelikož je jeho výsledek plně závislý na specifických okolnostech. Dle Úřadu však pro obdobné účely zpracování postačí vypracování jen jednoho balančního testu.[134]

K rozsahu zájmů a práv subjektů údajů posuzovaných v rámci testu Brejchová uvádí, že „*zájmy a základní práva subjektů údajů* [by měly být] *v rámci testu vykládány široce* […] *Nejedná se tedy jen o základní práva a svobody ve smyslu, v jakém je chápe LPS (protože na ni pojem základní práva a svobody odkazuje), ale o jakékoliv relevantní zájmy subjektů údajů, včetně ekonomických*."[135]

Správce tedy provede balanční test, při kterém zohlední význam jeho oprávněného zájmu na straně jedné a dopadů zpracování na takto extenzivně vyložená práva subjektů údajů na straně druhé. Dle Pokynů 3/2019 musí primárně zvážit dvě skutečnosti, a to „*1) do jaké míry má monitorování vliv na zájmy, základní práva a svobody jednotlivců a 2) zda způsobuje porušení*

---

[133] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 10-11.

[134] Úřad pro ochranu osobních údajů. *Právní důvody zpracování.* [on-line]. 2018. Dostupné z: https://old.uoou.cz/pravni-duvody-zpracovani/d-27318/p1=4753

[135] BREJCHOVÁ, D. Článek 6 [Zákonnost zpracování]. In: UŘIČAŘ, M. Obecné nařízení o ochraně osobních údajů: komentář. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.

nebo negativní důsledky s ohledem na práva subjektu údajů.“[136] Při posuzovaní míry zásahu do práv subjektů v důsledku videodohledu lze zkoumat např. počet dotčených subjektů údajů či velikost sledované oblasti. Z Pokynů 3/2019 vyplývá, že existuje významný rozdíl mezi použitím „*dohledu pomocí videokamer v odlehlé oblasti (např. ke sledování volně žijících živočichů nebo k ochraně kritické infrastruktury, jako je rádiová anténa v soukromém vlastnictví)*“ a „*dohledu pomocí videokamer na pěší zóně nebo v nákupním středisku*“.[137]

Při balančním testu je dle recitálu č. 47 GDPR nutno vzít ohled také na přiměřené očekávání subjektů údajů, plynoucí z jejich vztahů se správcem a určit, „*zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít*.“ Dle Pokynů 3/2019 a stanoviska WP249 zaměstnanec většinou neočekává,[138] že by měl být na pracovišti monitorován.[139] Je tak nutno postupovat opravdu šetrně a dle stanoviska WP249 nejlépe zpracování omezit z místního i časového hlediska.[140]

4.3. Zásady zpracování osobních údajů

Kromě zajištění platného právního základu je pro zachování zákonnosti zpracování třeba dodržet i základní zásady zpracování osobních údajů, vymezené v čl. 5 GDPR.

Zásady korektnosti, zákonnosti a transparentnosti

Dle odst. 1 písm. a) výše uvedeného ustanovení musí být osobní údaje „*ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem*“. Toto písmeno tak stanoví hned tři zásady zpracování osobních údajů, na jejichž dodržování musí správce dohlédnout.

Zásadu zákonnosti lze navázat na již rozebraný čl. 6 GDPR, který stanoví podmínky zákonnosti zpracování ve formě taxativního výčtu jednotlivých právních titulů. Zákonnost není omezena jen na dodržení čl. 6 GDPR – k zachování zákonnosti zpracování nesmí porušit žádné jiné ustanovení GDPR a musí být v souladu s ostatními platnými právními předpisy, jak

---

[136] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 11.
[137] Tamtéž. S. 12.
[138] Ve srovnání s např. návštěvníkem banky či zákazníkem u bankomatu.
[139] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 13.
[140] Pracovní skupina zřízená podle článku 29. *Stanovisko 2/2017 ke zpracování údajů na pracovišti*. [on-line]. 2017. Dostupné z: https://ec.europa.eu/newsroom/article29/items/610169/en. S. 8.

evropskými, tak i vnitrostátními. Zásada zákonnosti by byla porušena i v případě narušení např. smluvní povinnosti či povinnosti mlčenlivosti.[141] V pracovněprávním kontextu by tak sledování zaměstnanců prováděné v rozporu s § 316 ZPr porušovalo i čl. 5 odst. 1 písm. a) GDPR.

Zásada korektnosti je z těchto zásad na první pohled nejvíce abstraktní; tento pojem nelze nalézt nikde jinde v GDPR. Z anglického znění GDPR však lze vypozorovat, že tato zásada je opět zmíněna v recitálu č. 39, který uvádí povinnost zpracovávat osobní údaje „*zákonným a spravedlivým způsobem*“.[142] Nejasnost tak vyplývá z českého překladu, kde byl pojem „fairly“ vyložen dvěma možnými způsoby. Zásadu korektnosti dle GDPR je tak možno chápat jako zásadu spravedlivého zpracování, či zpracování v dobré víře.[143] Dle Rámiše spočívá v tom „*aby zpracování údajů probíhalo tak, aby nikomu nebyla zbytečně činěna újma a bylo dbáno pokud možno zájmů všech zúčastněných osob*.“[144]

Nejvíce GDPR rozvádí zásadu transparentnosti, a to ve výše uvedeném recitálu č. 39 a detailně i ve svém čl. 12, který stanoví podmínky informování subjektů údajů o zpracování jejich osobních údajů. Z tohoto důvodu se této zásadě tato práce bude věnovat až v rámci rozboru čl. 12 GDPR a informační povinnosti správce.

Zásada účelového omezení

V čl. 5 odst. 1 písm. b) GDPR je obsažena další významná zásada zpracování osobních údajů, a to zásada účelového omezení. Dle ní musí být osobní údaje „*shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný*“.

Určení účelu zpracování je typicky hned prvním aktem, který musí správce provést před započetím zpracování osobních údajů. Teprve až po určení účelu zpracování může zkoumat, zda je dán některý z právních základů dle čl. 6 GDPR. Nebylo by totiž možné, že by správce kupříkladu

[141] NULÍČEK, M. Zásady zpracování osobních údajů [II. Zásada zákonnosti, korektnosti a transparentnosti]. In: NULÍČEK, M. a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.
[142] Srov. anglické znění čl. 5 odst. 1 písm. a) GDPR: „*Personal data shall be:… processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);*“ a anglické znění první věty recitálu č. 39 GDPR: „*Any processing of personal data should be lawful and fair*.“
[143] RÁMIŠ, V. Článek 5 [Zásady zpracování osobních údajů]. In: UŘIČAŘ, M., Obecné nařízení o ochraně osobních údajů: komentář. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.
[144] Tamtéž.

v rámci užití oprávněného zájmu jako svého právního základu vymezil svůj zájem jako nějakou skutečnost, která by nebyla v souladu s jím vybraným účelem zpracování.[145]

Dle Pokynů 3/2019 může v případě zpracování pomocí kamerového systému být účelem např. „*podpora ochrany majetku a jiných aktiv, podpora ochrany života a fyzické integrity jednotlivců, shromažďování důkazů pro občanskoprávní nároky*“. Naopak nedostatečně konkrétní by bylo zpracování založené „*pouze na účelu „bezpečnosti“ nebo „pro vaši bezpečnost“*“. Správce musí vymezit účel zpracování zvlášť pro každou jednotlivou kameru.[146] To může být relevantní kupříkladu, pokud některá z kamer je namířena pouze na majetek zaměstnavatele a jejím účelem tak může být pouze ochrana majetku a jiná zase na zvlášť nebezpečný úsek pracoviště, na kterém často dochází k úrazům. U této kamery by pak účelem mohla být ochrana zdraví a života zaměstnanců.

Pokud zpracování slouží v některém případě hned několika účelům, je dle WP203[147] nutno specifikovat všechny účely dostatečně určitě (tak, aby bylo možné posoudit zákonnost zpracování). V případě souvisejících účelů lze vymezit koncept „celkového účelu“, pod který spadají. Nelze však tuto možnost zneužívat a definovat účel zpracování příliš široce.[148]

Zásada minimalizace údajů

Od identifikovaného účelu se odvíjí i další zásady zpracování dle GDPR, jako je zásada minimalizace údajů. V té čl. 5 odst. 1 písm. c) GDPR omezuje zpracovávané osobní údaje na „*přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány*“. Osobní údaje tak musí svým charakterem a významem odpovídat účelu zpracování, přímo souviset s tímto účelem a být zpracovávány pouze v nezbytném rozsahu. Zároveň však není třeba osobní údaje minimalizovat až do bodu, ve kterém jejich rozsah nebude dostatečný k naplnění účelu zpracování.[149]

Tato zásada může být ve zkoumané problematice naplněna mj. omezením umístění či záběru kamer nebo omezením doby uložení záznamů.

---

[145] Např. pokud by zaměstnavatel vymezil svůj oprávněný zájem jako zájem na ochraně majetku, ale jako účel zpracování by uvedl zajištění bezpečnosti zaměstnanců.

[146] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 8.

[147] Pracovní skupina zřízená podle článku 29. *Stanovisko č. 3/2013 o účelovém omezení* [on-line]. 2013. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[148] Tamtéž. S. 16.

[149] RÁMIŠ, V. Článek 5 [Zásady zpracování osobních údajů]. In: UŘIČAŘ, M., *Obecné nařízení o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.

Zásada přesnosti

Čl. 5 odst. 1 písm. d) GDPR definuje zásadu přesnosti osobních údajů. Podle tohoto ustanovení musí být osobní údaje v rámci zpracování „*přesné a v případě potřeby aktualizované*“ a zároveň „*musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny*“. Tato zásada je promítnuta také v právech subjektů údajů na opravu a výmaz osobních údajů (viz čl. 16 a 17 GDPR).

V případě zpracování osobních údajů kamerovým systémem se tato zásada uplatní pouze u kamerových systémů se záznamem. K naplnění této zásady Úřad doporučuje zabezpečit systémy tak, aby bylo zamezeno možným změnám ze strany nepovolaných osob.[150]

Zásada omezení uložení

Relevantnější pro zpracování pomocí kamerového systému je zásada omezení uložení osobních údajů. Tato zásada, obsažená v čl. 5 odst. 1 písm. e) GDPR požaduje, aby osobní údaje byly „*uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány*“. Po uplynutí doby uložení nezbytné k dosažení účelu zpracování musí správce osobní údaje vymazat, případně anonymizovat.[151]

Doba uložení může být správcem stanovena konkrétně (např. 24 hodin), ale i relativně (např. po dobu trvání určité marketingové aktivity).[152] V případě zpracování pomocí kamerového systému na pracovišti bude typicky zvolena první varianta.

Doba bude vždy stanovena *ad hoc* s ohledem na účel zpracování. U kamerového systému musí být stanovena opět pro každou kameru zvlášť. Nelze tak objektivně určit, jaká doba uchování záznamů bude pro kamerový systém nejvhodnější, dle názoru Úřadu pro ochranu osobních údajů by ale neměla přesáhnout 72 hodin.[153] Dle Pokynů 3/2019 by v případě videodohledu za účelem ochrany majetku mělo k dosažení účelu stačit uchování po dobu 1-2 dní, delší pak v případě

---

[150] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 9.

[151] Jelikož v důsledku anonymizace přestanou naplňovat definici osobních údajů, srov. recitál č. 26 GDPR: „*Zásady ochrany osobních údajů by se proto neměly vztahovat na anonymní informace, totiž informace, které se netýkají identifikované či identifikovatelné fyzické osoby, ani na osobní údaje anonymizované tak, že subjekt údajů není nebo již přestal být identifikovatelným*.“

[152] NULÍČEK, M. a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

[153] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 9.

víkendu či delšího období svátků. Vždy je však nutno dobu uložení jasně vymezit a doložit její nezbytnost pomocí konkrétních důkazů. [154]

Pokyny 3/2019 také nabízejí alternativní řešení, jako je ukládání záznamů pomocí „černé skříňky“, ke kterým lze získat přístup pouze v případě incidentu nebo monitorování v reálném čase, během kterého se údaje neukládají vůbec. Opět je ale třeba zohlednit všechny okolnosti zkoumaného případu.[155]

Zásada integrity a důvěrnosti

Závěrečná zásada integrity a důvěrnosti vyplývá z čl. 5 odst. 1 písm. f) a stanoví, že osobní údaje musí být „*zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením*“.

Tuto zásadu konkretizuje čl. 32 GDPR, který stanovuje podmínky zabezpečení zpracování. Technickým a organizačním opatřením se věnuje také čl. 25 GDPR. Tato práce se tak zásadě integrity a důvěrnosti bude věnovat až v dalších kapitolách v rámci výkladu výše uvedených ustanovení.

4.4. Povinnosti zaměstnavatele jakožto správce osobních údajů

Kromě dodržení jednotlivých principů zpracování a volby právního titulu zpracování musí zaměstnavatel jakožto správce osobních údajů dodržet i jednotlivé povinnosti, které mu stanoví GDPR.

4.4.1. Informační povinnost

Informační povinnost správce osobních údajů vychází z již zmíněné zásady transparentnosti, která dle recitálu č. 39 GDPR vyžaduje „*aby všechny informace a všechna sdělení týkající se zpracování těchto osobních údajů byly snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků*“.

---

[154] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2020. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en. S. 29.
[155] Tamtéž. S. 11.

Podrobněji je pak informační povinnost upravena v čl. 12 až 14 GDPR. Čl. 12 odst. 1 GDPR správci ukládá, aby přijal „*vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14*“.

Způsob a prostředky poskytnutí informací

Informace o zpracování osobních údajů musí být poskytnuty „*stručným, transparentním, srozumitelným a snadno přístupným způsobem*“. Tyto pojmy rozvádí výkladové pokyny WP260[156].

Dle článku 8 pokynů WP260 požadavek „stručnosti a transparentnosti“ splňuje taková informace o zpracování, která je především oddělena od ostatních, nesouvisejících informací. Podmínku transparentnosti by tak nemohla naplňovat např. informace o zpracování zasazená do smluvní dokumentace či obchodních podmínek. „Srozumitelnou“ je pak taková informace, které by měl rozumět průměrný subjekt údajů z těch, jejichž osobní údaje se v konkrétním případě zpracovávají. Povinností správce je tak odhadnout úroveň porozumění skupiny subjektů údajů a přizpůsobit tomu poskytovanou informaci o zpracování. Aspekt „snadné přístupnosti“ by se měl projevit v tom, že osoby by informace o zpracování neměly mít problém dohledat a mělo by jim být hned jasné, kde a jak informace zpřístupní.[157]

Základním principem zásady transparentnosti dle pokynů WP260 je, že „*subjekt údajů by měl být schopen předem rozpoznat rozsah a důsledky zpracování a neměl by být následně zaskočen tím, jak jsou jeho osobní údaje používány*.“[158] Také proto je v pokynech WP260 doporučeno zdůraznit především následky, ke kterým bude zpracování osobních údajů vést a rizika, která mohou subjektům údajů hrozit.[159]

Nakonec je nutno vyložit pojem „jasné a jednoduché jazykové prostředky“. Dle pokynů WP260 tento požadavek znamená, že informace by měly být co nejvíce konkrétní, bez použití neurčitých pojmů, a zároveň psané jednoduchým jazykem bez složitých obratů a dlouhých souvětí.[160]

---

[156] Pracovní skupina zřízená podle článku 29. *Pokyny k transparentnosti podle nařízení 2016/679* [on-line]. 2018. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31895
[157] Pracovní skupina zřízená podle článku 29. *Pokyny k transparentnosti podle nařízení 2016/679* [on-line]. 2018. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31895.
[158] Tamtéž.
[159] Tamtéž.
[160] Tamtéž.

Rozsah poskytovaných informací

GDPR stanoví rozsah povinně poskytovaných informací dle způsobu získání zpracovávaných osobních údajů. Před plněním informační povinnosti tak správce musí jasně určit, zda byly osobní údaje získány od samého subjektu údajů či z jiných zdrojů.[161]

Dle bodu 110 Pokynů 3/2019 se v případě sledování jedná o sběr osobních údajů přímo od subjektu údajů.[162] Pro určení rozsahu informační povinnosti se tak užije čl. 13 GDPR. Dle odst. 1 tohoto ustanovení je v rámci poskytovaných informací vždy třeba poskytnout údaje o totožnosti správce, jeho kontaktní údaje a totožnost případných příjemců osobních údajů a následně účel spolu s právním základem zpracování. Při užití právního titulu oprávněného zájmu je třeba dále tento oprávněný zájem specifikovat, další údaje je také potřeba uvést při existenci pověřence pro ochranu osobních údajů či při úmyslu správce předávat osobní údaje do třetích zemí.[163]

Odst. 2 článku 13 GDPR následně ukládá poskytnout další údaje, pokud jsou „*nezbytné pro zajištění spravedlivého a transparentního zpracování*“. Toto kritérium není dále rozebráno v GDPR ani v pokynech W260, nicméně je třeba se přiklonit k názoru, že je tyto údaje třeba uvádět až na jedinečné případy vždy.[164] Pro rozebíraný případ zpracování prostřednictvím kamerového systému na pracovišti je z údajů uvedených v čl. 13 odst. 2 GDPR relevantní především doba uložení osobních údajů a informace o právech subjektů údajů.[165]

Forma poskytnutí informací

Požadovaná forma poskytovaných informací je upravena v již zmíněném článku 12 odst. 1 GDPR. Jako základ je tímto ustanovením stanovena písemná forma. GDPR připouští ale i ústní předání informací, a to za podmínky, že si tuto formu konkrétní, správcem identifikovaný subjekt údajů přímo vyžádá. Ústní forma se však vzhledem k širokému rozsahu poskytovaných údajů a obtížnosti následného ověření informací nezdá jako vhodný prostředek.[166]

---

[161] Srov. čl. 13 a 14 GDPR.
[162] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf. S. 26.
[163] Tzn. mimo Evropský hospodářský prostor a Velkou Británii.
[164] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Praha: Wolters Kluwer, 2019. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-587-3. S. 242.
[165] Práva subjektů údajů budou rozebrána v následující kapitole této práce.
[166] Vhodné by bylo např. poskytnutí informací v písemné formě a následně ústní vysvětlení na požádání.

V případě informování o zpracování osobních údajů prostřednictvím kamerového systému navrhují Pokyny 3/2019 tzv. vícevrstvou metodu poskytování informací, kdy nejdůležitější informace by byly uvedeny v první vrstvě, v tomto případě na informační tabuli umístěné před vstupem do monitorovaných prostor. Pokyny 3/2019 mezi tyto údaje kromě samotného upozornění na kamerové monitorování[167] řadí informace o správci, účelu a právním titulu zpracování a o právech subjektů údajů, dále pak o nejvýznamnějších dopadech zpracování. Informační tabule by měla také zahrnovat odkaz na druhou vrstvu informační povinnosti např. ve formě QR kódu.[168]

Dle Návrhu metodiky je třeba do první vrstvy zahrnout i údaj, zda je kamerový systém se záznamem či bez záznamu.[169] Nicméně je stále třeba pamatovat, že taková infomační tabule by měla být především čitelná a jasně srozumitelná. Podrobněji rozebrat jednotlivé informace tak Návrh metodiky doporučuje ve druhé vrstvě, která může mít formu webové stránky či písemného dokumentu dostupného ve snadno přístupném místě.[170]

Tento podrobnější dokument pak musí obsahovat veškeré údaje, které jsou předmětem informační povinnosti dle GDPR, i když byly již poskytnuty v první vrstvě. Musí se jednat o komplexní dokument, ze kterého bude subjekt údajů schopen zjistit všechny potřebné informace o zpracování. Subjekt údajů tak mimo jiné získá možnost informovaně vykonávat práva, která mu přiznává GDPR.

4.4.2. Umožnění výkonu práv subjektů údajů

Právy subjektů údajů se GDPR zabývá ve svých článcích 15 až 22[171], v nichž přiznává právo na přístup k osobním údajům, právo na opravu a výmaz osobních údajů, na omezení zpracování a na přenositelnost osobních údajů. Dále umožňuje subjektům údajů vznést námitku proti zpracování jejich osobních údajů založených na právních základech veřejného a oprávněného zájmu. Nakonec má subjekt údajů také právo nebýt předmětem rozhodování založeného výlučně na automatizovaném zpracování jeho osobních údajů.

---

[167] Např. ve formě piktogramu kamery a nápisu „Dohled pomocí videokamer“.

[168] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf. S. 26.

[169] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 10.

[170] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 10.

[171] Mezi práva subjektů údajů lze řadit také čl. 12-14 GDPR, tzn. právo na poskytnutí informací o zpracování, ze kterého plyne již výše rozebraná informační povinnost správce. Čl. 12 GDPR také upřesňuje proces vyřizování žádostí subjektů údajů dle čl. 15-22 GDPR.

Většina těchto práv se vztahuje k osobním údajům, které správce uchovává. Z povahy věci tak nebudou uplatnitelná v případě zpracování osobních údajů pomocí kamerových systémů bez záznamu.

Právo na přístup k osobním údajům

Právo subjektu údajů na přístup k osobním údajům sestává ze dvou rovin. V první rovině má dle čl. 15 odst. 1 GDPR subjekt údajů právo požadovat od správce potvrzení, zda dochází ke zpracování jeho osobních údajů. Pokud zpracování skutečně probíhá, má subjekt údajů následně právo získat přístup ke zpracovávaným údajům ve formě kopie a obdržet další informace o zpracování či podat námitku k dozorčímu úřadu.[172]

Při zpracování osobních údajů prostřednictvím kamerových systémů bez záznamu se toto právo uplatní jen omezeně. Správce nemůže subjektu údajů poskytnout kopii zpracovávaných údajů, jelikož žádné osobní údaje neukládá. Má sice stále povinnost poskytnout potvrzení, avšak dle Pokynů 3/2019 „*jakmile uplyne okamžik monitorování v reálném čase, může … poskytnout pouze informaci o tom, že se žádné osobní údaje již nezpracovávají*“.[173]

V případě použití kamerových systémů se záznamem může pak subjekt uplatnit své právo v plné míře a získat tak kopii pořizovaného záznamu. Problém však nastává ve chvíli, kdy se na videozáznamu objeví další identifikovatelné osoby, jelikož dle čl. 15 odst. 4 GDPR nesmí být právem na poskytnutí kopie nepříznivě dotčena práva třetích osob. Správce by tak měl před poskytnutím záznamu zavést přiměřená technická opatření, např. rozostřením či rozmazáním záznamu anonymizovat ostatní zaznamenané osoby.[174] Neanonymizovanou kopii záznamu by mohl správce poskytnout žadateli, který prokáže, že má od všech dotčených osob souhlas s obdržením jejich osobních údajů.[175]

Správce však není povinen požadavku na přístup k osobním údajům vyhovět vždy – v případě nepřiměřených nebo zjevně nedůvodných žádostí může v souladu s čl. 12 odst. 5 GDPR buď subjektu údajů uložit administrativní poplatek či požadavek zcela zamítnout.[176]

---

[172] Viz čl. 15 GDPR.
[173] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf. S. 22.
[174] Tamtéž.
[175] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 13.
[176] Pokud je schopen nedůvodnost či nepřiměřenost prokázat.

Právo na opravu osobních údajů

Jak vyplývá z čl. 16 GDPR, správce má povinnost na žádost subjektu údajů bez zbytečného odkladu opravit jakékoli nepřesné osobní údaje, které se subjektu údajů týkají. Toto právo se dotkne opět pouze kamerových systémů se záznamem, a to s ohledem na povahu sbíraných osobních údajů jen ve výjimečných případech.[177]

Právo na výmaz osobních údajů

Subjekt údajů má dle čl. 17 GDPR také právo podat žádost o výmaz svých osobních údajů. Správce má povinnost této žádosti vyhovět, pokud je dán jeden z důvodů uvedených v čl. 17 odst. 1 GDPR, zejména pokud zpracování osobních údajů je protiprávní, již není účelné, subjekt údajů vznesl námitku[178] nebo odvolal svůj souhlas se zpracováním. Žádosti musí být vyhověno bez zbytečného odkladu, přesná délka lhůty není v GDPR specifikována a měla by záležet na skutkových okolnostech případu.[179]

Správce by měl zajistit, aby byl schopen žádostem o výmaz vyhovět bez zbytečného odkladu, což v případě pořizování většího množství videozáznamů může být obtížné. Lze se řídit doporučeními obsaženými v bodu 3.4.3 Návrhu metodiky a zpřístupnit subjektům údajů formulář žádosti o výmaz, jehož vyplnění umožní správci subjekt údajů na záznamu spolehlivě nalézt.[180]

Existují však i okolnosti, za kterých správce může žádost o výmaz osobních údajů zamítnout. Dle čl. 17 odst. 3 GDPR není nutno žádosti vyhovět, pokud je zpracování nezbytné mj. pro splnění právní povinnosti či k určení, výkonu nebo obhajobě právních nároků správce. Správce tak nemá povinnost vymazat např. videozáznam zachycující trestný čin na žádost jeho pachatele. V případě žádosti o výmaz z důvodu podání námitky subjektem údajů může správce pokračovat ve zpracování také tehdy, pokud jeho oprávněný zájem převažuje nad zájmem subjektu údajů.

---

[177] Jelikož videozáznam je ze své podstaty pravdivým odrazem skutečnosti a nemůže tak obsahovat nepřesné osobní údaje. Využití tohoto práva si lze představit pouze v situaci, kdy došlo k záměrné manipulaci s videozáznamem.
[178] Právo subjektu údajů vznést námitku proti zpracování osobních údajů v souladu s čl. 21 GDPR bude rozebráno dále v této práci.
[179] RÁMIŠ, V. Článek 17 [VII. Lhůta pro provedení výmazu]. In: UŘIČAŘ, M. *Obecné nařízení o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.
[180] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 14.

Je třeba také zmínit, že v případě videozáznamů lze žádosti o výmaz osobních údajů provést i jinak, než smazáním celého záznamu. Pokyny 3/2019 připouští i možnost rozmazání obrazu žadatele bez možnosti obnovení.[181]

Právo na omezení zpracování

Právo na omezení zpracování úzce souvisí s právem na výmaz osobních údajů. Uplatní se především v situacích, kdy nejsou naplněny důvody pro výmaz osobních údajů, anebo je úplné smazání pro subjekt údajů neúčelné.[182]

Pro úspěšnost žádosti o omezení zpracování je však stále třeba naplnit jeden z důvodů, vymezených v čl. 18 odst. 1 GDPR. Zejména se bude jednat o případy, kdy je zpracování protiprávní, ale subjekt údajů odmítá přistoupit k výmazu, nebo již nenaplňuje účel, avšak subjekt údajů osobní údaje potřebuje k určení, výkonu nebo obhajobě svých právních nároků.

K omezení zpracování osobních údajů lze přistoupit také po vznesení námitky subjektem údajů, pokud stále není jasné, zda oprávněný zájem správce na pokračování ve zpracování převažuje nad zájem subjektu údajů či nikoliv. Po vyhodnocení střetu zájmů pak dojde buď k výmazu osobních údajů či k zrušení omezení zpracování, o čemž musí správce subjekt údajů informovat.[183]

Při vyhovění žádosti o omezení zpracování uchovává správce osobní údaje beze změny. K jinému zpracování může dojít jen dle čl. 18 odst. 2 GDPR, a to „*se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Unie nebo některého členského státu*“.

Právo na přenositelnost údajů

Na rozdíl od jiných práv subjektů údajů, právo na přenositelnost údajů nebylo upraveno v předchozí právní úpravě na ochranu osobních údajů a zavádí ho až GDPR.[184] Dle pokynů WP242

---

[181] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf. S. 24.
[182] RÁMIŠ, V. Článek 18. In: UŘIČAŘ, M. *Obecné nařízení o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.
[183] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 14-15.
[184] RÁMIŠ, V. Článek 20. In: UŘIČAŘ, M. *Obecné nařízení o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.

„*Přenositelnost údajů subjektům údajů v podstatě umožňuje získat a opětovně používat ‚své' údaje pro své vlastní účely a napříč různými službami. Toto právo usnadňuje schopnost snadno a bez zábran přesouvat, kopírovat nebo předávat osobní údaje z jednoho informačního prostředí do jiného*."[185]

Toto právo se týká pouze osobních údajů získaných přímo od subjektu údajů a umožňuje tomuto subjektu údajů získat od správce své osobní údaje ve „*strukturovaném, běžně používaném a strojově čitelném formátu*".[186] Těžiště tohoto práva a jeho odlišení od práva na přístup lze shledat právě ve vymezení formátu poskytovaných údajů. V případě zpracování pomocí kamerových systémů tak toto právo spíše nenalezne uplatnění, jelikož u osobních údajů v podobě videozáznamu postačí poskytnutí kopie na základě práva na přístup.[187]

Právo vznést námitku

Subjekt údajů se může vymezit vůči zpracování založenému na veřejném zájmu či na oprávněném zájmu správce vznesením námitky proti zpracování. Správce poté osobní údaje nemůže dále zpracovávat, pokud neprokáže, že je zpracování nezbytné pro uplatnění právního nároku či pro závažné oprávněné důvody ke zpracování, které musí převažovat nad oprávněnými zájmy subjektu údajů.[188]

Pokud správce není schopen výše uvedené prokázat, musí zpracování okamžitě ukončit. Subjekt údajů pak také může žádat o výmaz osobních údajů.

Toto právo se také uplatní spíše v případech zpracování pomocí kamerových systémů se záznamem. Lze si ale představit i situaci, kdy subjekt údajů podá námitku i na zpracování prostřednictvím on-line monitorování. Dle Pokynů 3/2019 by tak subjekt údajů musel učinit hned „*při vstupu do monitorované oblasti, během pobytu v ní, nebo po jejím opuštění*". Správce by pak měl povinnost okamžitě ukončit monitorování.[189]

---

[185] Pracovní skupina zřízená podle článku 29. *Pokyny týkající se práva na přenositelnost údajů* [on-line]. 2017. Dostupné z: https://ec.europa.eu/newsroom/article29/items/611233

[186] Viz čl. 20 odst. 1 GDPR.

[187] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 15.

[188] Viz čl. 21 GDPR.

[189] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf. S. 24.

4.4.3. Vedení záznamů o činnostech zpracování

Při provádění zpracování osobních údajů má správce také povinnost vést záznamy o činnostech zpracování.[190] V praxi se jedná o písemný[191] dokument, který by měl obecně popsat každé konkrétní zpracování a poskytnout tak přehled o činnosti správce v daném případě.[192]

Čl. 30 odst. 1 GDPR stanoví výčet údajů, které musí záznam o zpracování obsahovat, a to mimo jiné identifikační údaje správce, účely zpracování a kategorie subjektů údajů či typy zpracovávaných osobních údajů. Správce by měl také uvést všechny případné příjemce osobních údajů, lhůty uložení osobních údajů a přijatá opatření k zabezpečení zpracování.

Tato povinnost se neuplatní plošně na všechny správce osobních údajů. Dle čl. 30 odst. 5 GDPR vést záznamy o činnostech zpracování nemusí podniky s méně než 250 zaměstnanci. Pro uplatnění této výjimky však platí další podmínky, a to že zpracování nesmí představovat pravděpodobné riziko pro práva a svobody subjektů údajů, musí být pouze příležitostné a zároveň nikdy nesmí zahrnovat zvláštní osobní údaje a údaje o trestních rozsudcích a trestných činech.

Tato kritéria musí být splněna kumulativně a v praxi je jen těžko představitelná situace, kdy by je zpracování splňovalo. Obzvlášť v případě zpracování pomocí kamerových systémů se jistě nebude jednat pouze o příležitostné zpracování a lze i tvrdit, že by takové zpracování pravděpodobně mohlo představovat riziko pro práva subjektů údajů.[193] Z tohoto důvodu je třeba doporučit vedení záznamů o činnostech zpracování každému zaměstnavateli bez ohledu na čl. 30 odst. 5 GDPR a počet jeho zaměstnanců.

4.4.4. Posouzení vlivu na ochranu osobních údajů

Před započetím zpracování osobních údajů musí správce také vyhodnotit, zda nemá povinnost v souladu s čl. 35 GDPR vypracovat posouzení vlivu nadcházejícího zpracování na

---

[190] Viz čl. 30 GDPR.
[191] Viz čl. 30 odst. 2 GDPR, za písemnou se považuje i elektronická forma.
[192] JAROLÍMKOVÁ, A. Článek 30 [II. Obecně k pojmu záznamů] In: UŘIČAŘ, M. *Obecné nařízení o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.
[193] MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer, 2019. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-587-3. S. 255-256.

ochranu osobních údajů. Dle čl. 35 odst. 1 GDPR musí posouzení vlivu provést vždy, když bude „*pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob*".

GDPR dále demonstrativně vymezuje určité situace, ve kterých bude zpracování vysoce rizikové a ve kterých je tak nutno vypracovat posouzení vlivu. Jedná se buď o rozsáhlé automatizované zpracování, na kterém je založeno rozhodování, či rozsáhlé zpracování zvláštních osobních údajů a údajů týkajících se trestních věcí a nakonec i „*rozsáhlé systematické monitorování veřejně přístupných prostorů*".[194]

Poslední zmíněný případ jistě souvisí se zpracováním osobních údajů pomocí kamerových systémů, jelikož ve většině situací půjde o „rozsáhlé systematické monitorování". V kontextu kamerových systémů na pracovišti však ne vždy půjde o monitorování veřejně přístupných prostorů; posouzení vlivu tak bude vždy nutné jen při sledování pracovišť, která jsou zároveň veřejným prostorem.[195] Toto samozřejmě neznamená, že při monitorování veřejně nepřístupných prostorů není nikdy třeba vypracovat posouzení vlivu, jelikož v této situaci zpracování osobních údajů může stále představovat vysoké riziko pro práva a svobody subjektů údajů v souladu s čl. 35 odst. 1 GDPR.[196]

Pro vyhodnocení, zda určité zpracování pravděpodobně představuje pro subjekty údajů vysoké riziko, je možno se řídit Seznamem druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů, který byl vypracován a zveřejněn Úřadem v souladu s čl. 35 odst. 4 GDPR.[197] Dle tohoto seznamu představuje zpracování pomocí kamerových systémů na pracovišti vysoké riziko např. pokud „*sledování zaměstnanců má určit jejich pohyb nebo sledovat průběžně jejich činnost*" a zároveň pokud dopadá na více než 20 zaměstnanců správce.[198] Další vodítko lze získat i z Návrhu metodiky, dle kterého je třeba

---

[194] Viz čl. 35 odst. 3 GDPR.
[195] Např. prodejny zboží, nikoli však veřejně nepřístupné kanceláře či sklady.
[196] Pracovní skupina zřízená podle článku 29. *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679* [on-line]. 2017. Dostupné z: https://ec.europa.eu/newsroom/article29/items/611236
[197] Dle čl. 35 odst. 4 GDPR „*Dozorový úřad sestaví a zveřejní seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů podle odstavce 1.*"
[198] Úřad pro ochranu osobních údajů. *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů* [on-line]. 2020. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940.

zpracovat posouzení vlivu „*v případě záměru zpracovávat biometrické údaje v rámci provozování kamerových systémů, a to zvláště na veřejně přístupných plochách*“.[199]

Povinnost vypracovat posouzení vlivu však může plynout i z jiných než výše uvedených situací a v každém případě je nutno pečlivě posoudit veškeré okolnosti konkrétního zpracování. Lze dokonce i doporučit, aby zaměstnavatel provedl posouzení vlivu pro každé zpracování prováděné pomocí kamerových systémů.[200]

Při vypracovávání posouzení vlivu je třeba se řídit rozsahem uvedeným v čl. 35 odst. 7 GDPR. Na rozdíl od záznamů o činnostech zpracování by posouzení vlivu mělo obsahovat i „*posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů*“ a „*posouzení rizik pro práva a svobody subjektů údajů*“. Správce by měl také uvést navrhovaná opatření k řešení vzešlých rizik. Pro podrobný postup při vypracovávání posouzení vlivu lze nahlédnout např. do Metodiky obecného posouzení vlivu na ochranu osobních údajů[201] zveřejněné Úřadem.

Je nutno také zmínit, že povinnost dle čl. 35 GDPR nekončí pouze vypracováním posouzení vlivu před započetím zpracování. Po celou dobu zpracování je třeba monitorovat dodržování opatření, řešících rizika a příslušně revidovat posouzení vlivu.[202]

4.4.5. Zajištění zabezpečení zpracování

Povinnost správce zavést vhodná opatření k zajištění zabezpečení zpracování a minimalizaci případných rizik pro práva a svobody subjektů údajů vyplývá ze zásady integrity a důvěrnosti[203] a je konkretizována v čl. 32 GDPR.

Toto ustanovení správci ukládá zavést „*vhodná technická a organizační opatření*“ k zajištění zabezpečení zpracování. Při výběru opatření má správce přihlédnout „*ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob*“. Dle GDPR je jedním z možných opatření také pseudonymizace a šifrování osobních údajů.[204]

---

[199] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 24.
[200] Posouzení vlivu je vhodné vypracovat za účelem dosažení co nejvyšší ochrany práv a svobod subjektů údajů, jelikož tento postup správci umožní identifikovat rizika a navrhnout opatření k jejich minimalizaci.
[201] Úřad pro ochranu osobních údajů. *Metodika obecného posouzení vlivu na ochranu osobních údajů* [on-line]. 2020. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940.
[202] Pracovní skupina zřízená podle článku 29. *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679* [on-line]. 2017. Dostupné z: https://ec.europa.eu/newsroom/article29/items/611236 . S. 16.
[203] Viz čl. 5 odst. 1 písm. f) GDPR.
[204] Viz čl. 32 odst. 1 GDPR.

Přijatá opatření by měla dle GDPR chránit především před zničením, ztrátou, změnou nebo neoprávněným šířením zpracovávaných osobních údajů, ať už k tomu dojde náhodně či v důsledku cíleného protiprávního jednání.[205]

Technická opatření

K zabezpečení zpracování osobních údajů je v první řadě nutno zavést vhodná technická opatření. V případě zpracování prostřednictvím kamerového systému rozlišují Pokyny 3/2019 fyzické zabezpečení systému a řízení přístupu k systému.[206] Fyzické zabezpečení systému může zahrnovat:

- ochranu před krádeží a manipulací ze strany neoprávněných osob, např. umístěním kamer mimo dosah běžných osob a umístěním jejich záznamového či zobrazovacího zařízení do zabezpečené místnosti;
- ochranu kanálů, prostřednictvím kterých je obraz z kamer šířen, mj. zabezpečením proti odposlechu;
- ochranu proti kybernetickým útokům pomocí firewallů, antivirů či jiných softwarových anebo hardwarových řešení;
- ochranu proti poruchám systému v podobě automatické detekce a oznámení poruch oprávněným osobám;
- ochranu proti ztrátě zpracovávaných osobních údajů po bezpečnostním incidentu, např. zálohy dat a jiné možnosti obnovy systému a jednotlivých údajů;
- ochranu před živly a jiným náhodným poškozením[207] hardwarovým zabezpečením systému.[208, 209]

Řízení přístupu k systému by mělo zajistit, aby ke kamerovému systému získaly přístup pouze předem určené oprávněné osoby a zabránit tak v přístupu všem třetím osobám. Řízení přístupu může být zajištěno následujícími opatřeními:

---

[205] Viz čl. 32 odst. 2 GDPR.
[206] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf. S. 33.
[207] Např. ve formě elektrického přepětí.
[208] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf. S. 33.
[209] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 21-22.

- zabezpečení místností se záznamovým či zobrazovacím zařízením kamerového systému, a to ve formě např. mříží na oknech, zabezpečených dveří s mechanickým či elektronickým zámkem či stálé ostrahy místnosti;
- fyzické natočení zobrazovacích zařízení tak, aby záběry či záznamy nebyly v dohledu nepovolaných osob;
- evidence přístupů jednotlivých uživatelů k systému a případně i jimi provedených změn a pravidelná kontrola těchto záznamů;
- ověřování a schvalování přístupu uživatelů k systému pomocí bezpečného technického řešení, např. ve formě dvoufázového ověření.[210]

Organizační opatření

K zabezpečení zpracování je kromě technických opatření třeba implementovat i organizační opatření, zajišťující především odbornost osob s přístupem ke kamerovému systému a jasně definované provozní postupy. Jednotlivá organizační opatření mohou zahrnovat:

- určení, který zaměstnanec je odpovědný za každodenní provoz kamerového systému, jeho opravy, obnovu či údržbu;
- odborná příprava jednotlivých pověřených zaměstnanců;
- postupy pro vyřizování žádostí subjektů údajů a třetích stran;[211]
- určení doby uložení videozáznamů, včetně rozdílných dob uložení v případě incidentů;
- pokyny pro plnění informační povinnosti dle GDPR.[212]

Výše uvedené výčty jednotlivých opatření nejsou zdaleka vyčerpávající – zaměstnavatel by se měl v každém jednotlivém případě zamyslet nad podmínkami, ve kterých je zpracování prováděno, a identifikovat konkrétní rizika, na která by se měl zaměřit. Inspirovat se při výběru opatření může také Návrhem metodiky, který ve svém oddíle 3.8 a násl. vymezuje podrobný postup pro určení rizikovosti zpracování pomocí kamerových systémů a volbu vhodných opatření k zamezení negativních dopadů.[213]

---

[210] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf. S. 33.
[211] Např. žádosti o přístup k videozáznamům, o výmaz osobních údajů atp.
[212] Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím* videotechniky [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf. S. 32-33.
[213] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 18-23.

4.4.6. Ohlašování a oznamování bezpečnostních incidentů

Pokud i přes přijatá technická a organizační opatření dojde k porušení zabezpečení osobních údajů[214], nastane bezpečnostní incident. Ihned po bezpečnostním incidentu musí správce vyhodnotit, zda toto konkrétní porušení zabezpečení osobních údajů může pravděpodobně představovat riziko pro práva a svobody fyzických osob.[215] Při posouzení rizika je třeba vzít v potaz především typ porušení zabezpečení, povahu a množství dotčených osobních údajů a možné následky incidentu. Důležitým faktorem je také snadnost zjištění totožnosti subjektů údajů v případě neoprávněného šíření osobních údajů.[216] Pokud je riziko nepravděpodobné[217], je dostačující incident zdokumentovat a pokud možno napravit jeho důsledky.

Pokud je riziko narušení práv a svobod fyzických osob pravděpodobné, správci přistupuje v souladu s čl. 33 odst. 1 GDPR povinnost incident ohlásit dozorovému úřadu[218]. Ohlášení incidentu by mělo být učiněno bez zbytečného odkladu, a to nejpozději do 72 hodin od okamžiku, kdy se správce o porušení zabezpečení dozvěděl, případně i později s uvedením legitimních důvodů pro zpožděné ohlášení. Je přípustné i postupné plnění ohlašovací povinnosti s postupným dodáváním jednotlivých údajů o incidentu.[219]

GDPR také stanoví minimální náležitosti ohlášení, a to ve svém čl. 33 odst. 3. Správce tak v komunikaci s dozorovým úřadem musí přinejmenším popsat porušení zabezpečení osobních údajů včetně výčtu kategorií a množství dotčených subjektů údajů a osobních údajů, uvést jméno a kontaktní údaje pověřence pro ochranu osobních údajů, pokud byl jmenován, popsat pravděpodobné následky incidentu a opatření přijatá správcem k jejich minimalizaci.

Pokud správce při vyhodnocování rizika po proběhnutí bezpečnostního incidentu shledá, že fyzickým osobám hrozí ve výsledku porušení zabezpečení jejich osobních údajů dokonce vysoké riziko, musí vedle ohlášení incidentu dozorovému úřadu uvědomit o incidentu i subjekty údajů, a to bez zbytečného odkladu.[220] Příkladem porušení zabezpečení, které nese vysoké riziko, může být neoprávněné šíření nebo zpřístupnění velkého množství zvlášť citlivých osobních údajů.

---

[214] Dle čl. 4 odst. 12 GDPR je *„porušením zabezpečení osobních údajů“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů“*

[215] Viz čl. 33 odst. 1 GDPR.

[216] Pracovní skupina zřízená podle článku 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [on-line]. 2018. Dostupné z: https://ec.europa.eu/newsroom/article29/items/612052/en

[217] Např. pokud byly neoprávněně šířené osobní údaje bezpečně zašifrované a je nepravděpodobné, že by se nepovolané osoby mohly dostat k originálům údajů.

[218] Dozorovým úřadem je na území České republiky Úřad pro ochranu osobních údajů.

[219] Viz čl. 33 odst. 1 a 4 GDPR.

[220] Viz čl. 34 odst. 1 GDPR.

V případě zpracování pomocí kamerových systémů může jít např. o šíření záznamů, obsahujících biometrické osobní údaje.

Oznámení subjektům údajů musí obsahovat přinejmenším stejné údaje, které musí obsahovat ohlášení dozorovému úřadu, s výjimkou popisu kategorií a počtu dotčených subjektů údajů a osobních údajů.[221]

Této oznamovací povinnosti se správce může vyhnout přijetím vhodných opatření, která přiměřeně sníží riziko hrozící právům a svobodám dotčených fyzických osob. Kontaktovat každou jednotlivou dotčenou osobu také nemusí, pokud by to vyžadovalo nepřiměřené úsilí. V takovém případě může správce oznamovací povinnost splnit prostřednictvím veřejného oznámení[222], např. na svých webových stránkách nebo v médiích.

Závěrem je třeba správci doporučit se již předem připravit na možnost proběhnutí bezpečnostního incidentu, a to předchozím nastavením pravidel a postupů pro ohlašování i oznamování incidentů, vyhodnocování rizik a vedení evidence případů porušení zabezpečení osobních údajů.[223]

4.4.7. Jmenování pověřence pro ochranu osobních údajů

Zaměstnavatelé, jejichž hlavní činnost ze své povahy, rozsahu nebo účelu vyžaduje provádění pravidelného, rozsáhlého a systematického monitorování subjektů údajů, by si měli být vědomi také povinnosti jmenovat pověřence pro ochranu osobních údajů, která vyplývá z čl. 37 odst. 1 GDPR.[224] Pověřencem je nutno jmenovat osobu s odbornými znalostmi práva a praxí v oblasti ochrany osobních údajů. Při volbě pověřence by měl správce zohlednit i schopnost potenciálního pověřence plnit úkoly související s jeho rolí.[225]

Dle čl. 39 GDPR má pověřenec pro ochranu osobních údajů na starosti zejména poskytování poradenství správci a zpracovatelům či zaměstnancům správce ohledně předpisů na ochranu osobních údajů a monitorování souladu činností správce s těmito předpisy. Úkolem

[221] Viz čl. 34 odst. 2 GDPR.
[222] Viz čl. 34 odst. 3 GDPR.
[223] Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873. S. 17-18.
[224] Povinnost jmenovat pověřence pro ochranu osobních údajů dopadá nejen na tuto kategorii správců, ale tato kategorie je pro účely této práce nejrelevantnější. Povinnost jmenovat pověřence mají např. i veřejné orgány nebo veřejné subjekty.
[225] Viz čl. 37 odst. 5 GDPR.

pověřence je také působit jako kontaktní osoba správce v komunikaci s dozorovým úřadem a spolupracovat s ním.

Lze doporučit jmenovat pověřence pro ochranu osobních údajů i zaměstnavatelům, na které se nevztahuje povinnost čl. 37 GDPR, obzvlášť zaměstnavatelům s velkým počtem zaměstnanců. Jmenování pověřence může zajistit vyšší stupeň ochrany osobních údajů subjektů údajů a zamezit případným porušením právních předpisů na ochranu osobních údajů.

Závěr

Cílem této diplomové práce bylo rozebrat právní úpravu spojenou s problematikou kamerových systémů na pracovišti a poskytnout přehled jednotlivých povinností, které z ní zaměstnavatelům vyvstávají.

V první části této práce byl přiblížen pojem „kamerový systém“ a byly vymezeny druhy kamerových systémů – atrapy kamer, kamerové systémy se záznamem a bez záznamu.[226] V souvislosti s tímto dělením bylo dovozeno, že i v případě kamerových systémů bez záznamu dochází ke zpracování osobních údajů, i když dle starších stanovisek Úřadu platil opak. Provozovatel kamerového systému bez možnosti ukládat záznam tak musí plnit povinnosti vyplývající z právních předpisů o ochraně osobních údajů.[227]

Druhá část této práce se zabývala českou pracovněprávní úpravou kontroly zaměstnanců na pracovišti, konkrétně prostřednictvím sledování. Z tohoto rozboru vyplynulo, že podmínky kontroly zaměstnanců, obsažené v ustanovení § 316 zákoníku práce, jsou vymezeny poměrně nepřesně a jsou plné neurčitých právních pojmů, jako je „přiměřený způsob kontroly“ či „zvláštní povaha činnosti zaměstnavatele“. Zkoumaná právní úprava může být pro zaměstnavatele nejasná, jelikož k dispozici nejsou žádná oficiální, snadno přístupná výkladová vodítka a různé prameny nabízejí protichůdné výklady výše uvedených pojmů. Zaměstnavatel tak může mít v praxi problém s dodržováním zákonných podmínek. Tuto situaci by bylo možné vyřešit například vydáním výkladové metodiky, kterou by se řídily i dotčené kontrolní orgány.

Obdobný problém se týká i informační povinnosti zaměstnavatele dle § 316 odst. 3 zákoníku práce. Konkrétně u informační povinnosti dochází k překryvu mezi její úpravou dle zákoníku práce a dle GDPR, přičemž informační povinnost dle GDPR je širší a přesněji vymezená. Nabízí se tedy otázka, zda ustanovení § 316 odst. 3 ZPr stále plní svůj účel a jestli nenadešel čas přizpůsobit českou právní úpravu té evropské.

Třetí část této práce se věnovala často opomíjené problematice atrap kamer na pracovišti. Tato práce nabízí překvapivý závěr, a to že i atrapy kamer mohou zasahovat do práv a svobod zaměstnanců. I pouhá iluze sledování, obzvlášť v soukromých prostorech pracoviště[228] narušuje právo zaměstnanců na příznivé pracovní prostředí a může vzbudit dojem zásahu do práva na soukromí. Jeden z problémů spočívá i v informační povinnosti, kterou s ohledem na nefunkčnost

[226] Kamerové systémy bez záznamu neukládají snímané video a poskytují pouze možnost on-line monitorování sledované oblasti.
[227] S výjimkou případů, kdy na záběrech kamery nejsou rozpoznatelné jednotlivé osoby.
[228] Na sociálních zařízeních, ale i třeba v šatnách, v prostorech určených k odpočinku apod.

atrap kamer není třeba plnit, nicméně z pohledu zaměstnanců[229] se může nesplnění této povinnosti ze strany zaměstnavatele jevit jako porušení zákona. V současnosti se oblastí atrap kamer zabývá jen minimum zdrojů a s ohledem na výše uvedené problémy je třeba doufat, že v budoucnu se to změní.

Ve čtvrté části této práce byla věnována pozornost obecnému nařízení o ochraně osobních údajů. Úvodem se tato část práce zabývala mj. výkladem jednotlivých právních základů zpracování osobních údajů. K tomuto je třeba zdůraznit, že v pracovním prostředí nelze spoléhat na právní titul souhlasu subjektu údajů. Aby byl souhlas se zpracováním platný, musí být mimo jiné dán svobodně – což v kontextu vztahu podřízenosti a nadřízenosti mezi zaměstnancem a zaměstnavatelem není ve valné většině případů možné. Zaměstnavatel tak musí užít zejména právní základ oprávněného zájmu, který s sebou však nese další povinnosti, např. vypracování balančního testu.

Těžištěm této části práce byl rozbor jednotlivých povinností, které GDPR spojuje se zpracováním osobních údajů pomocí kamerových systémů. Lze zhodnotit, že povinností souvisejících s instalací kamerového systému na pracovišti není málo a obzvlášť menší zaměstnavatelé by mohli mít problém se v nich zorientovat. Pomoci s plněním povinností dle GDPR mohou výkladové Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky[230], vydané Sborem. Ty však zejména pro laiky nemusí být snadno dohledatelné a srozumitelné. Je tak třeba doufat, že tuto mezeru zaplní Úřadem připravovaná Metodika ke kamerovým systémům.[231]

Stále ale chybí obdobný komplexní dokument k podmínkám kontroly zaměstnanců dle § 316 ZPr, který by jasněji vymezoval neurčité právní pojmy, použité v tomto ustanovení. Kromě vydání těchto výkladových pravidel by mohla být na místě i novelizace výše uvedeného ustanovení. Lze uvažovat především o vypuštění § 316 odst. 3 ZPr a přeformulování § 316 odst. 2 ZPr.

[229] Kteří předpokládají, že se jedná o funkční kamerový systém.
[230] Dostupné zde: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.
[231] Více k připravované metodice zde: https://old.uoou.cz/metodika%2Dke%2Dkamerovym%2Dsystemum%2Dzahajena%2Dverejna%2Dkonzultaced-56872

Seznam použitých zkratek

ESLP	Evropský soud pro lidská práva
EU	Evropská unie
Návrh metodiky	Návrh Metodiky ke kamerovým systémům
obecné nařízení o ochraně osobních údajů, 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
Pokyny 3/2019	Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky
Sbor	Evropský sbor pro ochranu osobních údajů
Úřad	Úřad pro ochranu osobních údajů
Ústav	Výzkumný ústav bezpečnosti práce
WP29	Pracovní skupina zřízená podle čl. 29 směrnice 95/46/ES
zákon o ochraně osobních údajů	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
zákoník práce, ZPr	Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
zpracování	zpracování osobních údajů

Seznam použitých zdrojů

1. Seznam použité literatury

HŮRKA, Petr. *Zákoník práce: komentář. 6. vydání*. Praha: Wolters Kluwer, 2020. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-910-9.

JANEČKOVÁ, Eva a BARTÍK, Václav. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde, 2011. Praktická právnická příručka. ISBN 978-80-7201-850-5.

JANEČKOVÁ, Eva a BARTÍK, Václav. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3.

KOTTNAUER, Antonín. *Zákoník práce: komentář*. Praha: Leges, 2012. Komentátor. ISBN 978-80-87576-08-3.

LANDWEHRMANN, T. *Zavedení kamerového systému na pracovišti (vzor směrnice)*. Praktická personalistika. ANAG, 2021(7-8), s. 35 – 42 ISSN:2336-5072

MORÁVEK, Jakub. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer, 2019. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-587-3.

NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

PICHRT, Jan. *Zákoník práce: Zákon o kolektivním vyjednávání*. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.

RAFAJOVÁ, Monika a VÁRYOVÁ, Lucia. *Biometrické osobné údaje podľa GDPR: (biometrický podpis, kamerový systém)*. Praha: Leges, 2019. Teoretik. ISBN 978-80-7502-433-6.

UŘIČAŘ, Miroslav. *Obecné nařízení o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-815-3.

VIDRNA, Jan a KOUDELKA, Zdeněk. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců*. V Praze: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7.

2. Seznam použitých internetových zdrojů

Evropský sbor pro ochranu osobních údajů. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [on-line]. 2019. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf

HEJNÁ, Veronika. *Inspektorát se zastal zaměstnanců. Atrapy kamer nelze používat jako nátlak na zaměstnance* [on-line]. 2022. Dostupné z: https://www.e15.cz/finexpert/vydelavame/inspektorat-se-zastal-zamestnancu-atrapy-kamer-nelze-pouzivat-jako-natlak-na-zamestnance-1390036

HEJNÁ, Veronika. *Kamerové systémy na pracovišti: Jaké má zaměstnavatel povinnosti?* [on-line]. 2020. Dostupné z: https://www.e15.cz/finexpert/vydelavame/kamerove-systemy-na-pracovisti-jake-ma-zamestnavatel-povinnosti-1371452

MÁLEK, Jakub a VESELÝ, Jakub. *Kamerové systémy na pracovišti a příznivé pracovní podmínky* [on-line]. 2022. pravniprostor.cz Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/kamerove-systemy-na-pracovisti-priznive-pracovni-podminky

Městský kamerový systém hlavního města Prahy [on-line]. 2022. Dostupné z: https://bezpecnost.praha.eu/clanky/kamerovy-system

NERAD, Libor. *Ochrana osobních údajů zaměstnance* [on-line]. 2022. epravo.cz. Dostupné z: https://www.epravo.cz/top/clanky/ochrana-osobnich-udaju-zamestnance-114436.html

NONNEMANN, František. *Vztahuje se GDPR i na on-line kamery?* [on-line]. 2020. epravo.cz Dostupné z: https://www.epravo.cz/top/clanky/vztahuje-se-gdpr-i-na-on-line-kamery-110746.html

PEJCHALOVÁ GRÜNWALDOVÁ, Vladimíra. *Evropský soud pro lidská práva: K zásahu do soukromí zaměstnanců* [on-line]. 2020. Dostupné z: https://advokatnidenik.cz/2020/03/19/evropsky-soud-pro-lidska-prava-k-zasahu-do-soukromi-zamestnancu/

SLOVÁČEK, Petr a HADAČ, Tomáš. *Velký bratr na silnicích: Kde všude číhají kamery? A kdo má k záznamům přistup?* [on-line]. 2021. Dostupné z: http://www.1227.cz/aktuality/velky-bratr-na-silnicich-kde-vsude-cihaji-kamery-a-kdo-ma-k-zaznamum-pristup

Výzkumný ústav bezpečnosti práce. *Odraz Obecného nařízení o ochraně osobních údajů v oblasti bezpečnosti a ochrany zdraví při práci a ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance*. 2020. [on-line]. Dostupné z: https://vubp.cz/soubory/produkty/publikace-ke-stazeni/odraz-gdpr-v-oblasti-bezpecnosti-a-ochrany-zdravi-pri-praci-a-ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance.pdf

Stanoviska a jiné zdroje z rozhodovací praxe Úřadu pro ochranu osobních údajů

Úřad pro ochranu osobních údajů. *Anonymizovaný protokol o kontrole (UOOU-04151/20-16)* [on-line]. 2021. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=55777

Úřad pro ochranu osobních údajů. *Desatero omylů*. [on-line]. Dostupné z: https://old.uoou.cz/desatero-omylu/ds-4818/archiv=0

Úřad pro ochranu osobních údajů. *K provozování kamer a kamerových systémů* [on-line]. 2022. Dostupné z: https://old.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=29535&n=k%2Dprovozovani%2Dkamer%2Da%2Dkamerovych%2Dsystemu&p1=1099

Úřad pro ochranu osobních údajů. *K provozování kamerového systému na pracovišti* [on-line]. 2013. Dostupné z: https://old.uoou.cz/k-provozovani-kameroveho-systemu-na-pracovisti1/d-1742

Úřad pro ochranu osobních údajů. *Kamerová atrapa sice GDPR neporušuje, ale její instalace může být sankcionována* [on-line]. 2022. Dostupné z: https://old.uoou.cz/kamerova-atrapa-sice-gdpr-neporusuje-ale-jeji-instalace-muze-byt-sankcionovana/d-55810

Úřad pro ochranu osobních údajů. *Metodika obecného posouzení vlivu na ochranu osobních údajů* [on-line]. 2020. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940.

Úřad pro ochranu osobních údajů. *Návrh Metodiky ke kamerovým systémům* [on-line]. 2023. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=56873

Úřad pro ochranu osobních údajů. *Přepravní a dopravní společnost – Kontrola kamerového systému se zaměřením na zaměstnance společnosti (UOOU-04151/20)* [on-line]. 2021. Dostupné z: https://old.uoou.cz/prepravni-a-dopravni-spolecnost-kontrola-kameroveho-systemu-se-zamerenim-na-zamestnance-spolecnosti-uoou-04151-20/ds-7043/archiv=0&p1=5209

Úřad pro ochranu osobních údajů. *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů* [on-line]. 2020. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940.

Úřad pro ochranu osobních údajů. *Stanovisko č. 1/2006 - Provozování kamerového systému z hlediska zákona o ochraně osobních údajů* [on-line]. 2006. Dostupné z: https://old.uoou.cz/files/stanovisko_2006_1.pdf

Úřad pro ochranu osobních údajů. *Stanovisko č. 1/2016 - Umístění kamerových systémů v bytových domech* [on-line]. 2016. Dostupné z: https://old.uoou.cz/stanovisko-c-1-2016-umisteni-kamerovych-systemu-v-bytovych-domech/d-18866

Úřad pro ochranu osobních údajů. *Stanovisko č. 12/2012 - K použití fotografie, obrazového a zvukového záznamu fyzické osoby* [on-line]. 2012. Dostupné z: https://old.uoou.cz/files/stanovisko_2012_12.pdf

Úřad pro ochranu osobních údajů. *Stanovisko č. 3/2014 - K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti* [on-line]. 2014. Dostupné z: https://old.uoou.cz/stanovisko-c-3-2014-k-nadbytecnemu-vyzadovani-souhlasu-se-zpracovanim-osobnich-udaju-a-souvisejicimu-nespravnemu-plneni-informacni-povinnosti/d-11913/p1=1099

Úřad pro ochranu osobních údajů. *Zveřejnění fotografií pořízených kamerovým systémem* [on-line]. 2015. Dostupné z: https://old.uoou.cz/zverejneni-fotografii-porizenych-kamerovym-systemem/d-14880/p1=1099

Pokyny a stanoviska z činnosti Pracovní skupiny zřízené podle čl. 29 směrnice 95/46/ES

Pracovní skupina zřízená podle článku 29. *Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679* [on-line]. 2018. Dostupné z: https://ec.europa.eu/newsroom/article29/items/612052/en

Pracovní skupina zřízená podle článku 29. *Pokyny k souhlasu podle nařízení 2016/679*. [on-line]. 2018. Dostupné z: https://ec.europa.eu/newsroom/article29/items/623051/en

Pracovní skupina zřízená podle článku 29. *Pokyny k transparentnosti podle nařízení 2016/679.* [on-line]. 2018. Dostupné z: https://old.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31895

Pracovní skupina zřízená podle článku 29. *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679* [on-line]. 2017. Dostupné z: https://ec.europa.eu/newsroom/article29/items/611236

Pracovní skupina zřízená podle článku 29. *Pokyny týkající se práva na přenositelnost údajů.* [on-line]. 2017. Dostupné z: https://ec.europa.eu/newsroom/article29/items/611233

Pracovní skupina zřízená podle článku 29. *Stanovisko 2/2017 ke zpracování údajů na pracovišti*. [on-line]. 2017. Dostupné z: https://ec.europa.eu/newsroom/article29/items/610169/en

Pracovní skupina zřízená podle článku 29. *Stanovisko 2/2017 ke zpracování údajů na pracovišti*. [on-line]. 2017. Dostupné z: https://ec.europa.eu/newsroom/article29/items/610169/en.

Pracovní skupina zřízená podle článku 29. *Stanovisko č. 3/2013 o účelovém omezení.* [on-line]. 2013. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Pracovní skupina zřízená podle článku 29. *Stanovisko č. 6 /2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES.* [on-line]. 2014. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf

3. Seznam použitých právních předpisů

Nařízení EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů

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

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

4. Seznam použité judikatury

Rozsudek Nejvyššího správního soudu ze dne 8. 11. 2011, č. j. 2 As 45/2010- 68

Rozsudek Nejvyššího soudu ze dne 16. 08. 2012, sp. zn. 21 Cdo 1771/2011

Rozsudek Nejvyššího správního soudu ze dne 23. 08. 2013, sp. zn. 5 As 158/2012 – 49

Rozsudek Nejvyššího soudu ze dne 26. 11. 2015, sp. zn. 21 Cdo 4596/2014

Rozsudek Velkého senátu ESLP ze dne 5. září 2017 ve věci 61496/08 – Bărbulescu proti Rumunsku

Rozsudek Velkého senátu ESLP ze dne 17. října 2019 ve věcech č. 1874/13 a 8567/13 – López Ribalda a ostatní proti Španělsku

5. Seznam ostatních zdrojů

Důvodová zpráva k zákonu č. 262/2006 Sb., zákoník práce

Rozhodnutí oblastních inspektorátů práce (viz část Příloha)

Příloha

Přílohu k této práci tvoří 4 rozhodnutí oblastních inspektorátů práce, která byla autorce práce poskytnuta na základě žádosti dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

1) Příkaz Oblastního inspektorátu práce pro hlavní město Prahu pod sp. zn. S3-2020-49
2) Příkaz Oblastního inspektorátu práce pro Ústecký a Liberecký kraj pod sp. zn. S7-2020-171
3) Rozhodnutí Oblastního inspektorátu práce pro Jihomoravský a Zlínský kraj pod sp. zn. S9-2019-323
4) Příkaz Oblastního inspektorátu práce pro Jihomoravský a Zlínský kraj pod sp. zn. S9-2020-373

Kamerové systémy na pracovišti

Abstrakt

Tato diplomová práce se věnuje problematice kamerových systémů na pracovišti, a to jak z pohledu českých pracovněprávních předpisů, tak z pohledu evropského obecného nařízení o ochraně osobních údajů. Práce se zaměřuje na analýzu jednotlivých právních pramenů a představuje přehled zákonných povinností a kritérií, které je zaměstnavatel k instalaci a užívání kamerových systémů na pracovišti povinen splnit.

Práce je rozdělena do čtyř tematických částí. V první části práce je věnován prostor definici pojmu „kamerových systém“ a dělení kamerových systémů na druhy dle kritérií, relevantních z hlediska právní úpravy ochrany osobních údajů. Následně je s důrazem na vývoj názoru Úřadu pro ochranu osobních údajů zkoumáno, zda vymezené druhy kamerových systémů spadají do působnosti GDPR. V této části je také vymezen pojem „atrap“ kamer.

Druhá část práce je zaměřena na výklad § 316 zákoníku práce, který upravuje možnost sledování zaměstnanců na pracovišti. Těžištěm této části práce je právní rozbor neurčitých právních pojmů ve zkoumaných ustanoveních zejména s pomocí odborné literatury, stanovisek Úřadu pro ochranu osobních údajů i rozhodnutí inspektorátu práce.

Třetí část práce se věnuje atrapám kamer na pracovišti a možným dopadům, které mohou představovat pro práva a svobody zaměstnanců. Tato část představuje průlomové rozhodnutí inspektorátu práce a vytyčuje potenciální problémy, se kterými se zaměstnavatel může setkat, pokud zvolí instalaci atrap kamer.

Čtvrtá část diplomové práce rozebírá obecné nařízení o ochraně osobních údajů a jeho užití v problematice kamerových systémů. V této části jsou s pomocí pokynů a stanovisek evropských poradních orgánů vyloženy klíčové pojmy a principy GDPR, dále se práce věnuje kritériím a povinnostem, které z něj vyplývají pro provozovatele kamerového systému na pracovišti.

Klíčová slova: kamerové systémy, sledování zaměstnanců, ochrana osobních údajů

CCTV systems in the workplace

Abstract

This thesis focuses on the topic of CCTV systems in the workplace, both from the perspective of Czech labour laws and the european General Data Protection Regulation. The thesis focuses on the analysis of individual legal sources and presents an overview of the legal obligations and criteria that the employer is obliged to fulfil in order to install and use CCTV systems in the workplace.

The thesis is divided into four thematic parts. In the first part of the thesis, space is devoted to the definition of the term "CCTV system" and the division of CCTV systems into types according to criteria relevant to the legal regulation of personal data protection. Subsequently, with emphasis on the development of the opinion of the Personal Data Protection Office, it is examined whether the defined types of CCTV systems fall within the scope of the GDPR. This section also defines the concept of 'dummy' cameras.

The second part of the thesis focuses on the interpretation of Section 316 of the Labour Code, which regulates the possibility of employee surveillance in the workplace. The focus of this part of the thesis is a legal analysis of legal terms in the examined provisions, in particular with the help of specialized literature, opinions of the Personal Data Protection Office and decisions of the Labour Inspectorate.

The third part of the thesis focuses on dummy cameras in the workplace and the possible impact they may have on the rights and freedoms of employees. This part presents a groundbreaking decision of the Labour Inspectorate and outlines the potential problems that an employer may encounter if they choose to install dummy cameras.

The fourth part of the thesis discusses the General Data Protection Regulation and its application to CCTVs. In this part, the key terms and principles of the GDPR are laid out with the help of guidelines and opinions of European advisory bodies, and the thesis also looks at the criteria and obligations that arise from it for the operator of a CCTV system in the workplace.

Keywords: CCTV systems, employee surveillance, personal data protection