ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Katedra pracovního práva a práva sociálního zabezpečení

DIPLOMOVÁ PRÁCE

Kamerové systémy na pracovišti

Natálie Lokajová

Plzeň, 2024

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Natálie LOKAJOVÁ**
Osobní číslo:	**R19M0226P**
Studijní program:	**M0421A220004 Právo a právní věda**
Téma práce:	**Kamerové systémy na pracovišti**
Zadávající katedra:	**Katedra pracovního práva a práva sociálního zabezpečení**

Zásady pro vypracování

1. Úvod
2. Právo na ochranu soukromí zaměstnanců na pracovišti
3. Kamerové systémy se záznamem na pracovišti
4. Problematika kamerových systémů bez záznamu na pracovišti
5. Judikatura a dosavadní praxe
6. Právní úprava de lege ferenda
7. Závěr

Rozsah diplomové práce:
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

- viz příloha

Vedoucí diplomové práce: **JUDr. Eva Ambrož Benešová, Ph.D., LL.M.**
Katedra pracovního práva a práva sociálního zabezpečení

Datum zadání diplomové práce: **9. ledna 2023**
Termín odevzdání diplomové práce: **31. března 2024**

Západočeská univerzita v Plzni
L.S.
Právnická fakulta

JUDr. et PhDr. Stanislav Balík, Ph.D.
děkan

Doc. JUDr. Jakub Morávek, Ph.D.
vedoucí katedry

V Plzni dne 5. září 2023

PROHLÁŠENÍ

„Prohlašuji, že jsem tuto diplomovou práci zpracoval samostatně, a že jsem vyznačil prameny, z nichž jsem svou práci čerpal způsobem ve vědecké práci obvyklým.“

V Plzni, 31. března 2024

Natálie Lokajová

PODĚKOVÁNÍ

Ráda bych tímto poděkovala JUDr. Evě Benešové, LL.M., Ph.D. za vedení této diplomové práce, vstřícnost a poskytování cenných rad při jejím zpracování. Dále bych chtěla poděkovat své rodině a blízkým lidem za bezbřehou podporu po celou dobu studia.

OBSAH

SEZHAM POUŽITÝCH ZKRATEK

SEZNAM POUŽITÝCH ZKRATEK

Právní předpisy, mezinárodní smlouvy a další prameny[1]

Evropská úmluva pro lidská práva	Sdělení č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto úmluvu navazujících
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/676 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
Kontrolní řád	Zákon č. 255/2012 Sb., o kontrole (kontrolní řád)
Listina EU	Listina základních práv Evropské unie
Listina základních práv a svobod	Usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, Předsednictva České národní rady
Metodika	Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů, 2024
MSDS	Městský kamerový dohlížecí systém
Občanský zákoník	Zákon č. 89/2012 Sb., občanský zákoník
Směrnice 95/46/ES	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 14. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
Správní řád	Zákon č. 500/2004 Sb., správní řád
Trestní zákoník	Zákon č. 40/2009 Sb., trestní zákoník
Úmluva č. 108	Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních údajů

[1] Není-li uvedeno jinak, jsou všechny předpisy v textu citovány ve znění pozdějších předpisů

Ústava ČR	Ústavní zákon č. 1/1993 Sb., Ústava České republiky, České národní rady
Zákon o inspekci práce	Zákon č. 251/2005 Sb., o inspekci práce
Zákon o odpovědnosti za přestupky	Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich
Zákon o ochraně osobních údajů	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
Zákon o zpracování osobních údajů	Zákon č. 110/2019 Sb., o zpracování osobních údajů
Zákoník práce	Zákon č. 262/2006 Sb., zákoník práce

Instituce

ESLP	Evropský soud pro lidská práva
EÚ	Evropská unie
NS	Nejvyšší soud
NSS	Nejvyšší správní soud
ÚOOÚ	Úřad pro ochranu osobních údajů
WP29	Pracovní skupina zřízená podle článku 29 Směrnice 95/46/ES zabývající se otázkami na ochranu soukromí a osobních údajů do platnosti GDP

Úvod

V dnešní době se bezpečnost a ochrana na pracovišti stávají stále důležitějším tématem a to, ať už se jedná o malé firmy či velké mezinárodní korporace. Jedním z klíčových nástrojů, který napomáhá zlepšit bezpečnost pracovního prostředí, jsou kamerové systémy. Tyto systémy umožňují monitorovat a zaznamenávat různé aktivity zaměstnanců v reálném čase, což poskytuje podnikům nejen důležité informace pro ochranu jeho majetku, ale především slouží k ochraně zaměstnanců. V neposlední řadě nesmíme opominout ani to, že kamerové systémy hrají výraznou roli jako nástroj prevence trestných činů a dalších nebezpečných situací. Avšak monitorování zaměstnanců v pracovním prostředí sebou nese značná rizika, a to především s ohledem jeho velké zneužitelnosti zaměstnavatelem a možností zásahu do osobnostních, ústavně zaručených, práv zaměstnanců.

Cílem této diplomové práce bude provedení celkové analýzy využívání kamerových systémů v pracovním prostředí, zkoumání jejich účinnosti, přínosů a potenciálních rizik, která jsou s jejich užíváním spojena. Stejně tak má práce za cíl čtenáře seznámit s aktuální právní úpravou monitoringu zaměstnanců s akcentem na právní aspekty ochrany osobních údajů. V neposlední řadě by měla dávat doporučení de lege ferenda.

První kapitola této práce se bude zaměřovat na právo na ochranu soukromí zaměstnanců na pracovišti. Tento úvodní úsek práce představuje teoretický rámec problematiky, zahrnující jak právní aspekty, tak i etické otázky spojené s monitorováním zaměstnanců na pracovišti. Bude zkoumáno, jaká práva mají zaměstnanci na ochranu svého soukromí v pracovním prostředí, stejně jako v této kapitole budou vymezeny konkrétní pojmy důležité pro kontext této práce.

Druhá kapitola se bude zabývat kamerovými systémy se záznamem na pracovišti, a to především s ohledem na problematiku zpracování osobních údajů zaměstnanců, včetně etických dilemat, která jsou s používáním těchto systémů spojena.

Třetí kapitola bude zaměřena na kamerové systémy bez záznamu. Zde budou rozebrány výhody či nevýhody tohoto přístupu s porovnáním s kamerovými systémy se záznamem.

Čtvrtá kapitola se bude věnovat analýze judikatury a dosavadní praxe týkající se používání kamerových systémů na pracovišti s ohledem především na rozhodnutí českých soudů a veřejných orgánů.

Pátá část se bude zabývat Úřadem pro ochranu osobních údajů, a bude zde vymezena jeho působnost jako dozorčího orgánu v kontextu kamerových systémů.

V závěrečné šesté kapitole budou navrhnuty doporučení a případné změny pro právní úpravu v této oblasti, a to na základě analýzy provedené v předchozích částech práce.

Cílem této práce je poskytnout ucelený pohled na problematiku kamerových systémů na pracovišti a přispět k lepšímu porozumění právního a etického rámce používání těchto systémů.

1 PRÁVO NA OCHRANU SOUKROMÍ ZAMĚSTNANCŮ NA PRACOVIŠTI

1.1 Vymezení základních pojmů

1.1.1 Právo na ochranu soukromí obecně

Právo na ochranu soukromí jako takové se zrodilo na konci 19. století, a to v důsledku vynálezu a rozvoje fotografie. Fotografie jako taková totiž najednou přinesla možnost zachytit téměř okamžitě aktuální podobu jakékoliv osoby, čehož začala využívat především bulvární žurnalistika. Toto mělo za následek definování pojmu práva na soukromí v článku „*The Right to Privacy*“ vydaném v Harvard Law Review profesory práv S.D. Warren a L. D. Brandeis.[2]

Toto základní osobnostní právo je chráněno demokratickými státy po celém světě. Z tohoto důvodu jej právní státy zakotvují ve svých národních ústavách a zavazují se k jeho dodržování přistoupením k mezinárodním dohodám. Mezi nejvýznamnější z těchto dohod patří například Všeobecná deklarace lidských práv nebo Evropská úmluva pro lidská práva. V České republice je právo na soukromí na ústavní úrovni definováno v Listině základních práv a svobod, konkrétně pak v čl. 7, čl. 8, čl. 12 a čl. 13. Toto dále rozvíjí zákonná úprava v občanském zákoníku.

Obsahem práva na soukromí, tak jak jej chrání Evropská úmluva pro lidská práva je ochrana jednotlivce před zásahem veřejné moci do jeho soukromého a rodinného života, stejně tak jako i ochrana obydlí a korespondence. Tyto složky práva na soukromí dle judikatury ESLP od sebe nelze zcela oddělit, je nutno je tedy chápat jako celek, jehož účelem je zajištění autonomie jednotlivce. Úprava práva na soukromí je v Listině základních práv a svobod značně roztříštěnější, což ostatně můžeme vyvodit z rozsahu množství výše vyjmenovaných článků. Listina základních práv a svobod na ústavní úrovni nad výše zmíněné čtyři složky výslovně zakotvuje ale i právo na informační sebeurčení, jímž se budeme podrobněji věnovat v další podkapitole.

[2] WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *HARVARD LAW REVIEW*. 15. 12.1890n. l., **1890**(5), 193-220.

1.1.2 Právo na informační sebeurčení

Právo na informační sebeurčení se vyvinulo a začalo získávat svou formu v reakci na rostoucí digitalizaci a sběr osobních údajů zejména v posledních desetiletích, a to obzvláště v souvislosti s rozvojem internetu a informačních technologií.

Poprvé byl tento pojem použit a definován v rozhodnutí německého Spolkového ústavního soudu ze dne 15. 12. 1983[3], kdy byla posuzována ústavnost v souvislosti s procesem a uchováním dat shromážděných za účelem sčítání lidu. V tomto rozsudku německý Spolkový ústavní soud uvedl, že jednotlivec v moderní společnosti musí být před neomezeným sběrem, uchováváním, užitím a zveřejňováním informací o jeho osobě chráněn v rámci ústavně garantovaného práva na soukromí. Následkem nemožnosti kontroly jednotlivce nad poskytnutými daty a informacemi, které mohou být zveřejněny, uchovány nebo využity pro jiné účely, než pro které byly poskytnuty, by došlo k zásadnímu narušení jeho práv a svobod, a to v takové míře, že by se již nadále nemohlo hovořit o demokratické a svobodné společnosti.[4]

Tato specifická část práva na soukromí zahrnuje do svého rámce též právo na ochranu před shromažďováním dat, sledováním, hlídáním a pronásledováním především ze strany moci veřejné. Nutno podotknout, že ani zde nejde o ochranu zcela bezpodmínečnou. Zásah do tohoto práva jednotlivce musí však být podroben ústavněprávním testem proporcionality, v kontextu kamerových systémů též známým jako testem balančním[5], jemuž bude věnována pozornost v samostatné kapitole.

V našem právním řádu je právo na informační sebeurčení garantováno na ústavní úrovni Listinou základních práv a svobod, konkrétně v článku 10, odst. 3, kdy *„Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“*[6] Tento článek rozvíjí na zákonné úrovni především zákon o zpracování osobních údajů.

---

[3] Rozsudek německého Spolkového ústavního soudu ze dne 15.12.1983, sp. zn. BVerfGE 65,1. Odkazovaný v nálezu Ústavního soudu ze dne 22.3.2011, sp. zn. Pl. ÚS 24/10.
[4] Tamtéž.
[5] Viz kapitola 4.4.1.
[6] Usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, Předsednictva České národní rady, ve znění pozdějších předpisů.

V mezinárodní rovině bylo toto právo zakotveno jako samostatné členskými státy EU v Listině EU, konkrétně pak v článku 8. Tento článek stanovuje, že osobní údaje jednotlivce musí být zpracovány s jeho souhlasem, případně na základě jiného oprávněného důvodu stanoveného zákonem, korektně a k přesně stanovených účelům. Ke shromážděným osobním údajům musí mít jednotlivec přístup a též musí mít právo na jejich opravu. V posledním odstavci předmětného článku je potom zakotvena pravomoc nezávislého orgánu, který dohlíží nad dodržováním těchto pravidel.[7] Tímto nezávislým orgánem je v České republice Úřad pro ochranu osobních údajů.[8] Článek 8 je dále prováděn sekundárním právem EU, konkrétně přímo závazným nařízením obecně známým jako GDPR.[9]

1.1.3 Právo na ochranu soukromí zaměstnanců na pracovišti

V předchozí kapitole jsem se věnovala právu na ochranu soukromí obecně. Má ale jednotlivec právo na soukromí i v pracovněprávním rovině? Tato otázka je dle mého názoru zcela zásadní. Především v laické veřejnosti se můžeme setkat s názorem, že zaměstnanec právo na soukromí na pracovišti nemá. Opak je ale pravdou.

Soukromí je osobní sférou jednotlivce, o jejíž narušení může rozhodovat pouze sám jednotlivec. Jeho míra nezávisí však pouze a jen na jednotlivci, ale především na okolních podmínkách, které jsou tvořeny různorodými faktory. Je tedy zjevné, že jednotlivec bude disponovat vyšší mírou soukromí v uzavřeném prostoru svého obydlí, který sdílí jen se svými nejbližšími, v porovnání právě s prostředím jeho pracoviště. Zásadním kritériem je proto individuální hodnocení odlišení míry soukromí v konkrétních životních situacích a nastavení závazných norem pro potenciální zásahy do tohoto základního lidského práva.[10]

Ochrana soukromí zaměstnanců na pracovišti je v našem právním řádu zajištěna především na zákonné úrovni, a to ku příkladu zákoníkem práce, zákonem o zpracování osobních údajů, občanským zákoníkem, trestním

[7] Listina EU.
[8] Viz kapitola 5.
[9] Mezi další prameny mezinárodního práva zakotvující právo na informační sebeurčíme řadíme Úmluvu č. 108 ze dne 28. 1. 1981, jež poprvé definovala pojmy patřící pod ochranu osobních údajů jako bezprostředně závazné. Dále také Směrnici 95/46/ES ze dne 14. 10. 1995, která byla předchůdcem GDPR.
[10] NONNEMANN, František: Soukromí na pracovišti, Právní rozhledy. Č. 7/2015, s. 229.

zákoníkem či dokonce zákonem o inspekci práce. Tyto však nijak nedefinují pojem soukromí, spíše, než že dávají zaměstnavateli určitý právní rámec, ze kterého nesmí vybočit.

Zákoník práce jako klíčový pracovněprávní předpis uvádí, že *„Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.“*[11] Subsidiárně se k zákoníku práce využije občanský zákoník, který upravuje ochranu podoby a soukromí jednotlivce v § 84 - § 90. Jeho subsidiarita[12] je stanovena v § 4 zákoníku práce. Trestní zákoník ve své zvláštní části, konkrétně v § 180, upravuje základní skutkovou podstatu trestného činu neoprávněného nakládání s osobními údaji, v druhém odstavci speciální ve vztahu pracovněprávním. Tohoto trestného činu se může dopustit zaměstnavatel, který byť jen z nedbalosti neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje zaměstnance, čímž mu zároveň způsobí vážnou újmu na jeho právech.[13] Méně závažnými zásahy do soukromí zaměstnance na pracovišti se zabývá zákon o inspekci práce. Tento zákon stanovuje odpovědnost zaměstnavatele za přestupky, kterých se dopustil na zaměstnancích ve sféře jejich soukromí a osobnostních práv. Zaměstnavatel, ať už jako fyzická osoba, fyzická osoba podnikající či právnická osoba, se dopustí přestupku tím, že naruší soukromí zaměstnance na pracovišti způsobem uvedených v § 316, odst. 2 zákoníku práce, neinformuje zaměstnance o rozsahu kontroly a způsobech jejích provádění dle § 316, odst. 3 zákoníku práce či v rozporu s § 316, odst. 4 vyžaduje od zaměstnance informace, které bezprostředně nesouvisejí s výkonem jeho práce a se základním pracovněprávním vztahem. Za takovýto přestupek, spočívající v neinformování zaměstnance o rozsahu kontroly hrozí zaměstnavateli uložení pokuty do 100.000, - Kč, za ostatní poté do 1.000.000, - Kč.[14]

[11] § 316, odst. 2 zákoníku práce.
[12] Princip subsidiarity v pracovněprávních vztazích znamená, že normy občanského zákoníku se aplikují pouze tehdy, když zákoník práce nedostatečně nebo vůbec nereguluje určitou právní otázku. Občanský zákoník se tedy aplikuje až v případě, pokud nelze otázku řešit pomocí speciálních pracovněprávních norem.
[13] § 180, odst. 2 trestního zákoníku.
[14] § 11a a § 24a zákona o inspekci práce.

1.1.4 Kamerový systém

Kamerový systém je technologické zařízení nebo soubor technologických zařízení složený z několika klíčových komponentů, které umožňují provádění operací zpracování, řízení a zabezpečení celého systému.

Těmito operacemi rozumíme vytváření obrazu skutečného světa v definovaném použitelném formátu, přenos snímků v rámci systému, dále také zobrazení, zpracování a ukládání snímků. Řízení kamerového sytému spočívá zejména ve správě činností a některých údajů a připojení kamerového systému k jiným systémům. Tímto jiným systémem může být automatické rozpoznávání registračních značek při odjezdu z placeného parkoviště nebo také požární poplach. V neposlední řadě jsou součástí komponenty zajišťující zabezpečení pořízených dat. Zabezpečení je realizováno také prostřednictvím přijatých technických a organizačních opatření.[15]

Jak už obsah diplomové práce naznačuje, kamerové systémy dělíme na dva základní typy – kamerové systémy vybavené záznamovým zařízením a kamerové systémy bez pořizování záznamu. Jednotlivým druhům se budu podrobněji zabývat v dalších kapitolách této práce.

Kamerové systémy nejčastěji hlídají bezpečnost na veřejných prostranstvích ve městech, není tedy divu, že nejrozšířenějším druhem kamerového systému je tzv. městský kamerový dohlížecí systém.[16] MKDS je specifický druh kamerového systému, který má především funkci preventivní. Jeho instalace má sloužit k vytvoření bezpečných zón v exponovaných lokalitách jako jsou nádraží, náměstí či sídliště. Je důležité zmínit, že na provoz těchto kamerových systému jsou poskytovány státní finanční prostředky.[17]

V oblasti MKDS jsou stále více jako alternativy ke klasickému kamerovému systému využívány kamery mobilní. Nepopiratelným přínosem je možnost rychlé a nenákladné instalace této kamery přímo v místě, kde je to zrovna účelné.

---

[15] ÚOOÚ. *Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů* [online]. 2024 [cit. 2024-02-24]. Dostupné z: https://uoou.gov.cz/media/profesional/met-kamerove-systemy-web-08022024.pdf.

[16] Dále jen jako „MKDS“.

[17] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Kamerové systémy* [online]. [cit. 2024-02-24]. Dostupné z: https://www.mvcr.cz/clanek/kamerove-systemy.aspx.

V dnešní době už ale kamerové systémy neslouží pouze k dohlížení nad bezpečností v reálném čase. Jak bylo zmíněno výše, ke kamerovému systému lze připojit i systémy další, čímž dojde k podstatnému rozšíření jeho funkcí. Proto se stále více provozovatelů kamerových systémů přiklání k instalaci často dražší ale o to výkonnější a inteligentnější varianty. Důvodem je zejména vyšší efektivnost takových to vyspělých zařízení.

Například zvukové senzory v kamerách jsou schopné detekovat rizikové situace jako jsou střelba, křik nebo tříštění skla a v reálném čase na tyto zvukové jevy dokáží upozornit. Do kamerových systémů lze instalovat i reproduktor. Tato funkce je zatím využívána především soukromými bezpečnostními agenturami, ale její potenciál je velký především ve vztahu k MKDS. Pokud totiž dojde k upozornění osoby, která se dopouští protiprávního či jinak nežádoucího činu v reálném čase, je velmi pravděpodobné, že tato osoba činu zanechá. A to bez rozdílu toho, zda tak učiní přímo osoba sedící v monitorovacím středisku nebo bude upozornění přehráno automaticky nahranou hlasovou zprávou.[18]

Mezi technologicky nejpokročilejší systémy pak patří ty, které dokáží rozpoznat a identifikovat osoby za pomocí biometrických údajů. Biometrie je obor, který využívá charakteristických znaků jednotlivců pro zjištění totožnosti nebo ověření identity. Dle charakteristických rysů ji můžeme rozdělit na biometrii fyziologickou (otisk prstu, termogram obličeje, duhovka a sítnice oka) a biometrii chování (mimika obličeje a pohybu rtů, dynamika stisku kláves).[19] Těchto kamer, které jsou schopné rozpoznat obličej v současnosti přibývá, a to zejména pro jejich velkou výhodu v podobě rychlosti verifikace. V České republice je tato technologie od roku 2020 využívána na všech mezinárodních letištích s pravidelným leteckým provozem[20] a k jejímu zavedení přistupují i někteří větší zaměstnavatelé, především za účelem rozlišení kmenových zaměstnanců, zaměstnanců agentur a jiných osob vstupujících do prostoru pracoviště. Téma zavedení kamerových systémů využívající technologii rozpoznávaní obličejů bylo

[18] ZOULOVÁ, Lenka a Miloslav FIŠER. *Inteligentní kamery vidí i slyší. Chytré technologie mění česká města* [online]. 2023 [cit. 2024-02-24]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-inteligentni-kamery-vidi-i-slysi-chytre-technologie-meni-ceska-mesta-40450506.

[19] PAVLÍK, Pavel. Biometrie jako základ současné i budoucí identifikace a autentizace. *Kontakt*. 2007, (2), 427-430. ISSN 1212–4117.

[20] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů* [online]. 2019 [cit. 2024-02-25]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceni-letiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx.

hojně diskutováno ohledně zamezení vstupu nežádoucích osob na fotbalové stadiony, avšak k tomuto se ÚOOÚ vyjádřil zamítavě.[21]

Avšak jedním z nejdůležitějších atributů kamerového systému je prostor, který dokáže zabrat. Z tohoto důvodu je liché uvádět počet kamer, který v rámci svého provozu určitý provozovatel naistaloval.[22] Rozlišujeme proto kamery klasické otočné a kamery multisenzorové.

Klasické otočné kamery spadají mezi nejuniverzálnější kamery, které umožňují pracovníkovi monitorovacího střediska přiblížit si či oddálit požadovanou oblast zájmu, stejně tak jako tyto kamery umožňují rotaci o 360 ° kolem vlastní osy. Nevýhodou ale je, že při otočení či přiblížení na sledovaný objekt nelze sledovat ostatní části prostoru, které kamera jinak zabírá.[23]

Podstatně vyšší rozsah zabraného prostoru může pokrýt kamera multisenzorová. Tato kamera totiž současně pořizuje 360° záběr a zajišťuje tak plné pokrytí. I zde je možnost, aby si operátor jednotlivé objekty do detailu přiblížil, nicméně i po tomto přiblížení kamera na rozdíl od klasické otočné kamery stále nahrává celou monitorovanou oblast.[24] Další nespornou výhodou multisenzorových kamer je možnost jejich instalace v diskrétním režimu. V tomto režimu je kamera zapuštěna do stropu a nikdo tak nepozná, zda se jedná o kameru nebo světlo.

Trendem poslední doby jsou tzv. „*body-worn cameras*“ v českém překladu známé jako nositelné, osobní či tělové kamery. Tyto se poprvé objevily v Nizozemí už v roce 1997 a dnes jsou využívány především veřejnými složkami států po celém světě. Tělové kamery mají sloužit ke zvýšení bezpečnosti prostřednictvím prevence a deeskalace agrese a incidentů, dále také jako podpora

[21] ÚOOÚ. *ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech* [online]. 2019 [cit. 2024-02-25]. Dostupné z: https://m.uoou.cz/vismo/dokumenty2.asp?id=35541&n=uoou-k-nbsp-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech.

[22] ZOULOVÁ, Lenka a Miloslav FIŠER. Inteligentní kamery vidí i slyší. Chytré technologie mění česká města [online]. 2023 [cit. 2024-02-24]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-inteligentni-kamery-vidi-i-slysi-chytre-technologie-meni-ceska-mesta-40450506.

[23] *Vysvětlení označení a zkratek při bezpečnostních kamerách* [online]. [cit. 2024-02-24]. Dostupné z: https://www.efeel.cz/vysvetleni-oznaceni-a-zkratek-pri-bezpecnostnich-kamerach.

[24] *KAMEROVÉ SYSTÉMY, NOVINKY, TECHNOLOGIE* [online]. [cit. 2024-02-25]. Dostupné z: https://www.securityblog.cz/2023/12/29/axis-predstavuje-inovativni-multisenzorove-kamery-s-umelou-inteligenci-pro-komplexni-pokryti-sirokych-ploch-v-rozliseni-az-4x4k/.

policejního vyšetřování.[25] Dle prováděných zahraničních výzkumů není ale pozitivní účinek těchto kamer zcela jednoznačný.[26]

1.1.5 Pracoviště zaměstnance

Zákoník práce se ve své úpravě zabývá třemi pojmy, a to pracovištěm, pravidelným pracovištěm a místem výkonu práce.[27]

Institut pravidelného pracoviště byl definován až s novelou zákoníku práce č. 365/2011 Sb., konkrétně byl pak zařazen jako § 34a zákoníku práce. Zákonodárce tímto institutem zavedl právní domněnku, cílící k ochraně zaměstnance před dosavadní aplikační praxí zaměstnavatelů, kdy bylo často pravidelné pracoviště sjednáno v takovém rozsahu, aby zaměstnavatel nemusel zaměstnanci poskytovat cestovní náhrady, čímž docházelo k poškozování práv zaměstnance.[28] Zákonná úprava zní, že *„Není-li v pracovní smlouvě sjednáno pravidelné pracoviště pro účely cestovních náhrad, platí, že pravidelným pracovištěm je místo výkonu práce sjednané v pracovní smlouvě. Jestliže je však místo výkonu práce sjednáno šířeji než jedna obec, považuje se za pravidelné pracoviště obec, ve které nejčastěji začínají cesty zaměstnance za účelem výkonu práce. Pravidelné pracoviště pro účely cestovních náhrad nesmí být sjednáno šířeji než jedna obec.“*[29]

Místo výkonu práce je na rozdíl od pravidelného pracoviště či pracoviště obligatorní náležitostí každé pracovní smlouvy. Avšak zákoníkem práce není toto nijak dále specifikováno. Z toho důvodu záleží zcela na projevech vůle obou stran smlouvy, jak široce či naopak konkrétně místo výkonu práce v pracovní smlouvě společně sjednají. Lze dokonce sjednat i více než jen jedno místo výkonu práce. Místem výkonu práce tak může být obec, kraj, organizační jednotka společnosti, dokonce i celá Česká republika, výjimkou ale není, že v pracovní smlouvě je

[25] ZEPCAM. *Výhody osobních kamer pro policii a orgány činné v trestním řízení* [online]. [cit. 2024-02-25]. Dostupné z: https://zepcam.com/cs/vyhody-telesnych-kamer-pro-policii-a-organy-cinne-v-trestnim-rizeni/.
[26] NATIONAL INSTITUTE OF JUSTICE. *Research on Body-Worn Cameras and Law Enforcement* [online]. 2022 [cit. 2024-02-25]. Dostupné z: https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement.
[27] Rozsudek NS ze dne 26. 11. 2015 sp. zn. 21 Cdo 4596/2014.
[28] Důvodová zpráva k zákonu 365/2011 Sb., kterým se mění zákon č. 262/2003 Sb., zákoník práce, ve znění pozdějších předpisů a dalších související zákony, bod 37.
[29] § 34a zákoníku práce.

sjednané místo výkonu práce zcela konkrétně, a to přesnou adresou, shodující se s provozovnou či sídlem zaměstnavatele.

Pojem pracoviště je na zákonné úrovni definován pouze speciálním zákonem ve vztahu k zákoníku práce, a to zákonem o inspekci práce. Tento zákon pojmem pracoviště rozumí „*místa určená nebo obvyklá pro výkon činnosti kontrolované osoby*[30]*, včetně jiného místa, než je pracoviště zaměstnavatele, je-li tam vykonávána práce na dálku nebo služba z jiného místa určená nebo obvyklá místa pro výkon činnosti kontrolované osoby*.“[31] Tuto definici pracoviště však nelze považovat v kontextu právního řádu za generálně použitelnou. Z tohoto důvodu lze výkladem dojít k tomu, že se obecně jedná o místo, kde zaměstnanec plní podle pokynů zaměstnavatele své pracovní úkoly a toto místo je omezeno sjednaným místem výkonu v pracovní smlouvě.[32] Zákoník práce pojem pracoviště výslovně používá zejména ve spojení s úpravou pracovní doby.[33] Specificky se tedy může jednat o prostor kanceláře, skladu nebo stavby, pracovištěm může být ale i například pro profesionálního řidiče prostor dopravního prostředku.

Ve vztahu k tématu diplomové práce je ale velice důležité zdůraznit, že prostor pracoviště je nutno vykládat extenzivně. Nejedná se jen o konkrétní přidělené pracovní místo, nýbrž také o prostor, který nezbytně s plněním pracovních úkolů a činností souvisí. Mezi takovéto prostory řadíme chodby, schodiště, prostory pro osobní hygienu, šatny a prostory určené k odpočinku či stravování zaměstnanců.[34] Avšak pro některé z těchto prostorů, jako třeba pro prostory pro osobní hygienu, platí striktnější pravidla pro zřízení kamerových systémů v porovnání s kancelářemi nebo sklady.

1.1.6 Kamerové sledování

Pojem kamerové sledování není v českém právním řádu definován. Kamerové sledování jako takové odkazuje na samotný proces monitorování událostí, aktivit nebo prostoru pomocí kamerového systému. Rozumí se jím

[30] Kontrolovanou osobou může být dle kontrolního řádu orgán moci výkonné, orgán územně samosprávného celku, jiný orgán a právnická nebo fyzická osoba.
[31] § 45 zákona o inspekci práce.
[32] Rozsudek NS ze dne 28. 11. 2015, sp. zn. 21 Cdo 4596/2014.
[33] BĚLINA, Miroslav. § 34a [Pravidelné pracoviště]. In: BĚLINA, Miroslav, DRÁPAL, Ljubomír a kol. Zákoník práce. 4. vydání. Praha: C. H. Beck, 2023, s. 232, marg. č. 4.
[34]HUBACZKOVÁ, Gabriela. *Pojem pracoviště z pohledu bezpečnosti práce* [online]. [cit. 2024-02-23]. Dostupné z: https://www.bozpinfo.cz/pojem-pracoviste-z-pohledu-bezpecnosti-prace.

využití dostupných technických prostředků ke generování nebo snímání obrazu, přenosu obrazu a zobrazení obrazu, případně společně obrazu se zvukem. Těmito technickými prostředky jsou tzv. CCTV[35], fotopasti nebo webkamery.[36]

V kontextu pracovněprávním jej lze chápat dle § 316, odst. 2 jako systematické delší dobu trvající nebo opakující se kontrolu zaměstnance ze strany zaměstnavatele pomocí kamerového systému. Nejedná se tedy o kontrolu jednorázovou.[37]

Zákoník práce v § 316 výslovně neuvádí pojem kamerového systému, tento paragraf představuje pouze demonstrativní výčet způsobů, kterými je zaměstnavatel oprávněn kontrolu zaměstnance provádět. A to jak v obecné rovině v podobě otevřeného nebo skrytého sledování či konkrétními nástroji jakými jsou odposlech, záznam telefonických hovorů, kontrola elektronické pošty a kontrola listovních zásilek adresovaných zaměstnanci. V tomto můžeme pozorovat určitý skrytý záměr zákonodárce, který pouze taxativně nevymezil možné nástroje kontroly. Nýbrž zde nechal prostor pro jejich budoucí rozšíření, bez nutnosti novely zákona, a to v podobě obecného pojmu skrytého nebo otevřeného sledování. Pod tento pojem můžeme zařadit právě zmíněné kamerové systémy, ale i další, v budoucnu vzniklé, technologické prostředky zajišťující kontrolu zaměstnanců na pracovišti.

1.1.6.1 Kamerové sledování bez zpracování osobních údajů

Kamerové sledování nemusí být nutně spojeno se zpracováním osobních údajů, a to i přes fakt, že současný právní rámec v oblasti zpracování osobních údajů v České republice chápe i online monitoring, který neuchovává žádný záznam, jako formu zpracování osobních údajů. Tomuto tématu se ale budeme podrobněji věnovat dále v diplomové práci.

Tato podkapitola má především za cíl čtenáři odhalit případy kamerového sledování při kterých nejsou zpracovávány osobní údaje, a tudíž nespadají do působnosti ÚOOÚ ani do oblasti GDPR.

---

[35] Zkratka CCTV, složená z anglického Closed Circuit Television, v překladu jako uzavřený televizní okruh, je používána ve stejném významu jako kamerový systém.

[36] ÚOOÚ. *Provozování kamerových systémů: Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů* [online]. [cit. 2024-02-24]. Dostupné z: http://www.promenybydleni.eu/metodika_provozovani_kamerovych_systemu.pdf.

[37] MORÁVEK, Jakub. KONTROLA A SLEDOVÁNÍ ZAMĚSTNANCŮ – VÝKLAD § 316 ZPR. Právní rozhledy [online]. Praha, 2017(17), 573 [cit. 2024-03-05]. Dostupné z: https://app.beck-online.cz/bo/chapterview-document.

Zpracování osobních údajů se totiž vztahuje pouze na situace, kdy lze přímo či nepřímo kamerovým sledováním konkrétní fyzickou osobu identifikovat.[38]

Výjimkou z působnosti dohledu ÚOOÚ tedy tvoří tzv. přehledové kamery[39], které jsou nejčastěji využívány městy k jeho propagaci či skiareály nebo plaveckými halami k přehledu zákazníka o momentálním počasí či aktuálním množství návštěvníků takovýchto areálů. Tyto jsou nejčastěji bez omezení veřejně dostupné na internetových stránkách města či daného areálu.

Další výjimkou z působnosti GDPR jsou videokamery instalované v autě s funkcí parkovacího asistenta, avšak tato kamera musí být nastavená tak, aby nezaznamenávala žádné informace týkající se konkrétních fyzických osob.[40] Mezi tyto kamery se neřadí kamery palubní instalované do automobilu za účelem ochrany majetku a zajištění důkazního materiálu pro orgány činné v trestním řízení. Dle ÚOOÚ se sice v případě palubních kamer nejedná o vysoce rizikové zpracování osobních údajů, ale v jiných státech EU lze za takto nainstalovanou kameru udělit i pokutu dle GDPR.

Mezi zpracování osobních údajů se konečně také nebude řadit ani kamerový sytém provozovaný fyzickou osobou, který zachycuje výlučně osobní či domácí činnosti, a to při současném splnění podmínky, že kamerový systém nesnímá veřejné prostranství.[41]

Působnost ÚOOÚ se rovněž nevztahuje na atrapy kamer.[42]

---

[38] Stupeň identifikace fyzické osoby je popsán v kapitole 2.1.6.2.

[39] BURIAN, David. ÚOOÚ. Seminář k metodice návrhu a provozování kamerových systémů [online]. 2024. s. 5 [cit. 2024-03-11]. Dostupné z: https://uoou.gov.cz/media/seminare-uoou/prezentace/2024-03-06-seminar-uoou-metodika-ke-kameram.pdf.

[40] Tamtéž.

[41] EUROPEAN DATA PROTECTION BOARD. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky [online]. 2020. s. 7-8. [cit. 2024-02-28]. Dostupné z: https://edpb.europa.eu/edpb_guidelines__video_devices_cs.pdf.

[42] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-02-29]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.
BURIAN, David. ÚOOÚ. Seminář k metodice návrhu a provozování kamerových systémů [online]. 2024. s. 5 [cit. 2024-03-11]. Dostupné z: https://uoou.gov.cz/media/seminare-uoou/prezentace/2024-03-06-seminar-uoou-metodika-ke-kameram.pdf.
Za kamerovou atrapu se označována imitace kamerového systému bez technologických funkcí, jež má za cíl vzbudit dojem kamerového sledování a v důsledku toho preventivně působit na potenciální pachatele.

1.1.6.2 Stupeň identifikace osoby

Jak již bylo řečeno v předchozí kapitole, o zpracování osobních údajů jde pouze v případě, že pomocí kamer lze rozeznat konkrétní fyzickou osobu. S tímto neodmyslitelně souvisí stupeň identifikace takovéto osoby.

ÚOOÚ pro účely Metodiky stanovil že „*Metodika využívá stupeň velikosti, jak je definuje norma ČSN EN 62676-4 Dohledové systémy pro použití v bezpečnostních aplikacích část – 4: Pokyny pro aplikace, tj. monitorování, zjištění, pozorování, rekognoskace, identifikace, prozkoumání pro určení, zda se jedná o zpracování či nikoliv.*“[43] Dle Metodiky je tedy za zpracování osobních údajů kamerovým monitoringem považováno, pokud vyobrazená osoba v záběru zabírá více než 25 % výšky obrazu, případně pokud na jeden pixel obrazu připadá méně než 40 mm reálné výšky postavy. Je důležité podotknout, že se jedná o minimální hodnoty, a protože většina kamer je v současnosti vybavena funkcí zoomu neboli přiblížení, musíme počítat i s tím, že v situaci, kdy obraz zobrazené osoby překročí tyto hranice i po přiblížení, jedná se o zpracování osobních údajů.[44]

Mezi další aspekty, které musí zaměstnavatel brát v úvahu při instalaci kamerového systému, jenž mohou ovlivnit možnost identifikace fyzické osoby na pracovišti patří zejména světelné podmínky. To však nemusí být až takový problém, protože většina dnes již dostupných kamerových systémů disponuje funkcí nočního vidění, které umožňuje identifikaci osob i při snížených světelných podmínkách. Dodatečně může mít vliv na identifikaci též nutné maskování pracovníka pomocí ochranných pomůcek jako jsou respirátory či ochranné brýle nebo například rychlost pohybu zaměstnance. To vše musí při instalaci kamerového systému zohledněno tak, aby bylo co nejvíce dosaženo stanoveného účelu instalace.

[43] Tamtéž. s.5.
[44] Tamtéž. s.7.

2 KAMEROVÉ SYSTÉMY SE ZÁZNAMEM NA PRACOVIŠTI

Kamerové systémy jsou v dnešní době hojně využívány jako forma prevence k ochraně majetku a osob. Umožňují kontrolu a monitoring oblastí střeženého prostoru a zajišťují přenos a uchování takto získaného záznamu. Kamerové systémy pak mohou být dobrým pomocníkem například při odhalování trestné činnosti. Při umístění na veřejných prostranstvích nebo ve veřejných budovách poté přispívají k zajištění klidného soužití občanů. Nejen v České republice, ale i v celém světě se množství kamerových systémů pozorujících nás na každém kroku rok od roku zvyšuje a s technickým pokrokem, který nám moderní doba přináší, se jejich funkce stále zdokonalují. Je tedy přirozené, že tyto systémy musí být veřejnou mocí právně regulovány, aby nedocházelo k jejich zneužívání. A to ať už ze strany samotné veřejné moci nebo, a právě především soukromých mezinárodních korporací, které mají ve světě stále větší hlas.

Z důvodu širokého využití, funkčnosti a v současné době už i cenové dostupnosti kamerových systémů jej začali využívat taktéž zaměstnavatelé na svých pracovištích. I zde dochází ke střetnutí dvou světů, jejichž zájmy si mohou odporovat. Zaměstnavatel instaluje kamerový systém zejména za účelem sledování a kontroly zaměstnanců, která si klade za cíl nejen zefektivnění práce zaměstnance, ale také dodržování vnitřních předpisů sloužících k zajištění bezpečnosti a ochrany zdraví zaměstnance při práci. Dalším účelem, kterým zaměstnavatel sleduje je ochrana jeho majetku.[45] Oproti zájmům zaměstnavatele poté stojí zájmy zaměstnanců jako osob sledovaných, kterým může být se zavedením monitorovacího systému kamer snadno zasahováno do jejich soukromé sféry. Nadměrná kontrola může mít za následek narušení důvěry ze strany zaměstnance, která může mít negativní dopad ve formě vytvoření nepříjemného pracovního prostředí plného stresových faktorů, což může být vyhodnoceno i jako porušení zákoníku práce. Konkrétně by mohlo dojít k porušení povinnosti vedoucích zaměstnanců vytvářet příznivé pracovní podmínky pro zaměstnance.[46]

[45] BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 3. vyd. Praha: Linde Praha, 2013. Praktická právnická příručka. ISBN 978-80-86131-96-2, s. 141.
[46] § 302 písm. c) zákoníku práce.

3 PROBLEMATIKA KAMEROVÝCH SYSTÉMŮ BEZ ZÁZNAMU NA PRACOVIŠTI

Kamerové systémy bez záznamu jsou zařízení, která mají schopnost snímat obrazový materiál, ale nenahrávají nebo neukládají tento materiál pro pozdější použití nebo analýzu. Tato zařízení mohou sloužit k monitorování nebo dočasnému sledování, ale nedisponující trvalou funkcionalitou záznamu. Jedná se tedy jen o jakýsi online přes obrazu.[47]

Problematikou kamerových systémů bez záznamu se zabýval ÚOOÚ poprvé v roce 2006. Ve stanovisku vydaném pod číslem 1/2006[48] ÚOOÚ konstatoval, že samotné kamerové sledování bez pořízení záznamu není zpracováním osobních údajů dle zákona o ochraně osobních údajů.[49] ÚOOÚ tento závěr aplikoval ve své dozorové praxi a dále jej specifikoval v dalších stanoviscích[50] a obecných dokumentech jim vydávaným.

Obecným dokumentem potvrzující tento postoj je Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů zaměřená na provozování kamerových systémů, [51] vydaná ÚOOÚ v roce 2012. V této metodice ÚOOÚ výslovně uvádí, že provozování kamerového sytému je považováno za zpracování osobních údajů jen při kumulativním splnění dvou podmínek. První podmínkou je provádění záznamu pořizovaného obrazového materiál, který může být v některých výjimečných případech doplněn záznamem zvukovým. Druhou podmínkou je naplnění účelu kamerového sledování, čímž se rozumí využití kamerových záznamů k identifikaci fyzických osob v souvislosti s jejich určitým jednáním.[52] Toto stanovisko bylo rovněž akceptováno a reflektováno českými soudy.[53]

---

[47] JANEČKOVÁ, Eva a Václav BARTÍK. *Kamerové systémy v praxi*. Linde Praha, 2011. ISBN 978-80-7201-850-5. s. 42.

[48] ÚOOÚ. *Provozování kamerového systému z hlediska zákona o ochraně osobních údajů* [online]. 2006 [cit. 2024-02-28]. Dostupné z: https://www.smocr.cz/Shared/Clanky/7086/stanovisko-uoou-c-1-2006.

[49] Tento zákon pozbyl účinnosti dne 23. 04. 2019 a byl nahrazen zákonem o zpracování osobních údajů.

[50] ÚOOÚ. *Umístění kamerových systémů v bytových domech* [online]. 2016 [cit. 2024-02-28]. Dostupné z: https://www.scmbd.cz/UOOU_Umisteni_kamerovych_systemu_v_bytovych_domech.

[51] ÚOOÚ. *Provozování kamerových systémů: Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů* [online]. [cit. 2024-02-24]. Dostupné z: http://www.promenybydleni.eu/metodika_provozovani_kamerovych_systemu.pdf

[52] Tamtéž.

[53] Rozsudek NSS ze dne 25. 02. 2015, č.j. 1 As 113/2012-133.

V důsledku přímého nařízení GDPR byla přijata českým zákonodárcem nová právní úprava toto nařízení zohledňující, proto dne 23. dubna 2019 pozbyl účinnosti zákon o ochraně osobních údajů, jenž byl z velké části přetransformován do zákona o zpracování osobních údajů, který nabyl účinnosti následujícího dne, tedy 24. dubna 2019. Tento zákon převzal definice pojmů jako osobní údaj a zpracování osobních údajů z předchozí právní úpravy, tudíž zůstala v platnosti i předchozí stanoviska ÚOOÚ.

Závěr shodující se stanoviskem 1/2006 potvrdil ÚOOÚ i ve své odpovědi z 13. září 2019. Na dotaz studentky zabývající se problematikou kamerových systémů bez záznamu ÚOOÚ sdělil, že *„Není-li pořizován záznam fyzických osob, nejedná se o zpracování osobních údajů ve smyslu obecného nařízení,*[54] *to se na daný postup nevztahuje a uvedení jednání neumožňuje ÚOOÚ uplatnit svěřenou dozorovou kompetenci.“*[55]

Nicméně praxe jiných nezávislých evropských úřadů dozorujících nad ochranou osobních údajů, tak jak jejich postavení zavedla Listina EU, není v tomto tématu sjednocena.

První potenciální vlaštovkou k postupné výkladové změně názoru ÚOOÚ byly pokyny 3/2019[56] Evropského sboru pro ochranu osobních údajů,[57] přijaté dne 29. ledna 2020. I když v těchto pokynech není explicitně vyjádřeno, že kamerové systémy bez záznamu jsou zpracováním osobních údajů, vyplývá to z obsahu některých bodů.

Takovýmto bodem je bod 11, který se zabývá výjimkou z osobní či domácí činnosti působnosti GDPR. V tomto bodě je uvedeno, že do oblasti působnosti GDPR nespadá takové zpracování osobních údajů, které je činěno fyzickou osobou výlučně v průběhu osobních či domácích činností, mezi které se mohou řadit i online činnosti. Dalším takovým bodem je bod 29, který uvádí, že

---

[54] GDPR.

[55] RÖSLEROVÁ, Karolína. *Sledování zaměstnanců v kontextu Obecného nařízení o ochraně osobních údajů*. Diplomová práce, vedoucí Morávek, Jakub. Praha: Univerzita Karlova, Právnická fakulta, Katedra pracovního práva a práva sociálního zabezpečení, 2020.

[56] Dále v textu jen jako „Pokyny“
EUROPEAN DATA PROTECTION BOARD. *Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky* [online]. 2020 [cit. 2024-02-28]. Dostupné z: https://edpb.europa.eu/edpb_guidelines_video_devices_cs.pdf.

[57] Jedná se o instituci EU, zřízenou GDPR, dříve označující se názvem „Pracovní skupina WP29“, sdružující zástupce nezávislých evropských úřadů dozorujících nad ochranou osobních údajů, včetně Evropského inspektora ochrany osobních údajů, jejímž cílem je jednotné uplatňování GDPR v zemích EU.

v některých případech může být nutné vedle kamerového monitoringu též provádět záznam, za jiných okolností však nikoli či je tomu naopak, z čehož vyplývá, že se v obou případech jedná o zpracování osobních údajů v režimu GDPR. Stejně tak jako bod 116 pak představuje vzor informační tabule, jež by měla upozorňovat na vstup do monitorované oblasti, přičemž podle tohoto vzoru by měla tabule obsahovat také informaci o tom, zda se jedná o online monitoring nebo kamerový systém se záznamem.[58]

Z těchto bodů tedy jasně vyplývá, že Evropský sbor pro lidská práva zastává na rozdíl od ÚOOÚ názor, že ať už se jedná o kamerové systémy se záznamem či bez záznamu, oba tyto druhy kamerových systémů zpracovávají osobní údaje zachycených osob.

K těmto pokynům vydal ÚOOÚ shrnutí.[59] Shrnutí ÚOOÚ se však vůbec nezabývá kamerovými systémy bez záznamu. Spíše než to, nabízí opravdu osekaný náhled do Pokynů 3/2019 se zaměřením především na otázku zákonnosti zpracování osobních údajů a práva dotčených osob.[60] Nejspíše i proto toto shrnutí ÚOOÚ není dnes již dohledatelné na oficiálních stránkách instituce.

Vlaštovka v podobě Pokynů tedy nevedla ke změně výkladu a ani odborná literatura zabývající se tématem kamerových systémů tento posun nezaznamenala. Příkladem může být odborná publikace *Nežádoucí chování na pracovišti*, vydaná v loňském roce, ve které je nadále uváděno, že pokud nedochází k pořizování záznamu, nejedná se o zpracování osobních údajů.[61] Obdobným příkladem může být i článek zveřejněný dne 21. ledna 2021 serverem Právo 21 v němž se píše, že z důvodu absence funkce ukládání záznamu u kamerových systémů bez záznamu nejsou tyto podřízeny režimu zpracování osobních údajů dle GDPR a zákona o zpracování osobních údajů, nýbrž jejich instalace náleží do působnosti

[58] EUROPEAN DATA PROTECTION BOARD. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky [online]. 2020 [cit. 2024-02-28]. Dostupné z: https://edpb.europa.eu/edpb_guidelines__video_devices_cs.pdf.

[59] ÚOOÚ. Shrnutí Pokynů 3/2019 ke zpracování osobních údajů prostřednictvím videozařízení [online]. [cit. 2024-02-29]. Dostupné z: https://www.helpgdpr.cz/rstsp/clanky.nsf.pdf.

[60] Vztahuje se GDPR i na online kamery? NONNEMANN, František. Epravo.cz [online]. 2020 [cit. 2024-02-29]. Dostupné z: https://www.epravo.cz/top/clanky/vztahuje-se-gdpr-i-na-online-kamery.

[61] ŠIMEČKOVÁ, Eva. Nežádoucí chování na pracovišti. Leges, 2023. ISBN 978-80-7502-698-9.s.22.

občanského zákoníku a Listiny základních práv a svobod.[62] Výjimkou je ale odborná publikace Jaroslava Zahradníčka nesoucí název *Ochrana osobnosti v pracovněprávních vztazích*, kterou autor vydal v roce 2019. V této knize si autor pokládá otázku, zda stanovisko ÚOOÚ[63], ve kterém ÚOOÚ uvádí, že pouhé kamerové sledování bez záznamu není zpracováním osobních údajů, obstojí i přes účinnost GDPR. Sám autor poté prezentuje svůj názor, že je rozhodným, s jakým záměrem je kamerový systém zaměstnavatelem provozován. Pokud je záměrem soustavný dohled nad zaměstnancem, jedná se autora o zpracování osobních údajů.[64]

Je nutné podotknout, že sám ÚOOÚ si začal názorový posun v oblasti online monitoringu připouštět, i přes vydané shrnutí. Také to bylo důvodem smazání některých ÚOOÚ dříve vydaných stanovisek.

Dne 8. února 2024 zveřejnil ÚOOÚ novou Metodiku k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů.[65] Tato metodika se věnuje nejen kamerovým systémům se záznamem, ale nově také říká, že i kamerové systémy bez záznamu podléhají dozorové činnosti ÚOOÚ.

[62] Instalace bezpečnostních kamer musí být v souladu s ochranou osobních údajů. MIKUŠOVÁ, Hana. Právo 21 [online]. 2021 [cit. 2024-02-29]. Dostupné z: https://pravo21.cz/pravo/instalace-bezpecnostnich-kamer-musi-byt-v-souladu-s-ochranou-osobnich-udaju.
[63] ÚOOÚ. Provozování kamerového systému z hlediska zákona o ochraně osobních údajů [online]. 2006 [cit. 2024-02-28]. Dostupné z: https://www.smocr.cz/Shared/Clanky/7086/stanovisko-uoou-c-1-2006.
[64] ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Praha: Leges, 2019. Teoretik. ISBN 978-80-7502-373-5. s. 203.
[65] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-02-29]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

4 PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ KAMEROVÝMI SYSTÉMY NA PRACOVIŠTI

Výsledkem nové Metodiky ÚOOÚ je sjednocený postup a požadavky na instalaci kamerových systémů bez záznamu a se záznamem. Obě tyto formy totiž dle Metodiky ÚOOÚ nově považuje za zpracování osobních údajů.[66] Samozřejmě i z tohoto platí výjimky, kdy se o zpracování osobních údajů jednat nebude. Některé z těchto výjimek jsou uvedeny v kapitole 2.1.6.1. Kamerové sledování bez zpracování osobních údajů této práce.

Je třeba mít na paměti, že zavedení kamerového systému na pracovišti se řídí obecně nejen evropským předpisem GDPR, ale též vnitrostátním zákonem o zpracování osobních údajů a v neposlední řadě též zákoníkem práce, který je k předchozím právním předpisům právní úpravou speciální.

Avšak jediným relevantním ustanovením pro kamerové systémy na pracovišti je v celém zákoníku práce pouze § 316, proto je většina pravidel pro zavedení monitoringu na pracovišti dovozována a vykládána na základě obecných principů.[67] Dokonalou ukázkou výkladu je právě nově vydaná Metodika ÚOOÚ, která sice není právně závazná, ale je adekvátním prostředkem pro nastavení kamer v souladu s právními předpisy.

§ 316 zákoníku práce se zaměřuje na oblast ochrany majetku zaměstnavatele a též na ochranu osobnostních práv zaměstnance. Oprávnění zaměstnatele ke kontrole a sledování zaměstnanců stanovuje bez rozdílu mezi těmi, kteří jsou ve vztahu k zaměstnavateli v základním pracovní poměru či jsou zaměstnáni na základě dohod konaných mimo pracovní poměr.[68]

---

[66] ÚOOÚ. Úřad pro ochranu osobních údajů zveřejnil novou Metodiku k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů. [online]. [cit. 2024-03-01]. Dostupné z: https://uoou.gov.cz/novinky/vse/nova-metodika-uradu-ke-kamerovym-systemum.

[67] HOSPODÁŘSKÉ NOVINY. Soukromí v práci ve světle evropské judikatury [online]. ZAHRADNÍČEK, Jaroslav. 2019 [cit. 2024-03-01]. Dostupné z: https://hn.cz/c1-66611530-soukromi-v-praci-ve-svetle-evropske-judikatury#viz8.

[68] MORÁVEK, Jakub. KONTROLA A SLEDOVÁNÍ ZAMĚSTNANCŮ – VÝKLAD § 316 ZPR. Právní rozhledy [online]. Praha, 2017(17), 573 [cit. 2024-03-01]. Dostupné z: https://app.beck-online.cz/bo/chapterview-document.

4.1 Základní zásady pro zpracování osobních údajů

Právní zásady jsou klíčové a regulativní ideje, které určují podobu a fungování celého právního systému. Jsou klíčové pro interpretaci a aplikaci práva. A ačkoliv jsou jen zřídka kdy výslovně uvedeny v právních předpisech jsou závazné. Jejich význam spočívá v tom, že slouží jako vodítka pro tvorbu a aplikaci právních norem, pomáhají soudcům při interpretaci právních předpisů a zajišťují konzistentnost a spravedlnost v právním prostředí.[69]

Základní zásady pro zpracování osobních údajů jsou explicitně uvedeny v článku 5, odst. 1 a 2 GDPR. Jak již bylo zmíněno v předchozím odstavci, je výjimečné, pokud jsou zásady uvedeny přímo v textu právní normy. GDPR ale v tomto navazuje na předchozí právní úpravu v podobě Úmluvy 108 a následné směrnice 95/46 ES.[70]

4.1.1 Zásada zákonnosti, korektnosti a transparentnosti

Zásada zákonnosti je alfou a omegou zpracování osobních údajů. Zajišťuje, že ke zpracování osobních údajů dojde zejména prostřednictvím taxativně vymezených právních titulů. Několik z těchto titulů, jež jsou významné pro oblast pracovněprávní budou rozebrány v kapitole 4.2.

Zásada korektnosti ukládá povinnost poctivého, ohleduplného a přiměřeného zpracování osobních údajů, přičemž je samozřejmě důležité posuzovat naplnění této zásady v konkrétním případě. Dle této zásady je podstatně vyloučeno získávat osobní údaje skrytou cestou, jakou může být například odposlech.[71]

Zásada transparentnosti poskytuje subjektům údajů právo na informační sebeurčení[72], tedy jejich právo rozhodnout se jaké údaje o sobě poskytnou.[73]

---

[69] ŠRAJ, Jan. Zásady činnosti veřejné správy [online]. Olomouc, 2013 [cit. 2024-03-31]. Dostupné z: https://theses.cz/id/m5e3e1/. Diplomová práce. UNIVERZITA PALACKÉHO V OLOMOUCI, právnická fakulta. Vedoucí práce JUDr. Ing. Filip Dienstbier, Ph.D.

[70] FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. GDPR: hmotné a procesní aspekty prakticky. V Praze: C.H. Beck, 2019. Právní praxe. ISBN 978-80-7400-762-0.s.5.

[71] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7. s. 39.

[72] Viz kapitola 1.1.2.

[73] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7. s. 39.

4.1.2 Zásada legitimního účelu

Zásada legitimního účelu stanovuje zaměstnavateli povinnost zpracovávat osobní údaje zaměstnanců získané pomocí kamerového systému, pouze k účelu předem stanovenému. Mezi tyto účely řadíme zvýšení ochrany majetku a zvýšení bezpečnosti osob.

Kamerové systémy na pracovišti mohou být instalovány i za účelem shromažďování a uchování důkazů pro případ pojistné události nebo trestního řízení, nicméně je nutné podotknout, že to nesmí být hlavním a jediným účelem instalace kamer. Vždy musí být naplněn účel buďto ochrany majetku nebo bezpečnosti osob.[74]

Stojí za připomínku, že zásada legitimního účelu není zásadou absolutní. Obecně z ní existují tři výjimky a to, souhlas dotčené osoby, právní předpis unijního nebo vnitrostátního práva to dovoluje pro cíle uvedené v článku 23 odst. 1 a článku 6 odst. 4 GDPR, další zpracování osobních údajů je v souladu s vědeckými nebo historickými účely dle článku 5 odst. 1, písm. b) GDPR.[75] Přičemž druhá výjimka musí obstát z hlediska testu slučitelnosti účelů.

4.1.3 Zásada minimalizace údajů

Tato zásada přináší povinnost zaměstnavatele sbírat a zpracovávat jen relevantní osobní údaje zaměstnance s důrazem na přiměřenost jejich rozsahu. V tomto případě je velice důležité určit, zda se jedná o zpracování osobních údajů z kamerového systému se záznamem či bez něj. Důvodem je odlišná intenzita rozsahu zpracovávaných údajů.

Pro dodržení této zásady je nutné podrobit kamerový systém balančnímu testu,[76] který zohlední faktory jako jsou: množství a umístění kamer, šířku záběru kamer, režim kamerového záznamu, nutnost rozšířených funkcí kamerového systému (zvukový záznam, reproduktor, biometrická detekce) a také dobu

[74] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-02]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.
[75] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7. s. 39.
[76] Viz kapitola 4.4.1.

uchování záznamu.[77] Tyto jsou následně vyhodnoceny tak, aby docházelo k co možná nejmenšímu zásahu do osobní sféry zaměstnance a zároveň bylo dosaženo účelu instalace kamerového systému.

4.1.4 Zásada přesnosti a aktuálnosti údajů

Zásada přesnosti stanovuje povinnost zaměstnavatele k nezbytnému zpracování přesných osobních údajů a též osobních údajů aktuálních.

V oblasti kamerových systémů je tato zásada vztažena na požadavky omezení možnosti neautorizovaných změn jako je střih nebo neoprávněná manipulace se systémem a pořizování záznamu v takové kvalitě, jež umožňuje identifikaci.[78]

4.1.5 Zásada omezení doby uchování údajů záznamu

Z této zásady vyplývá závazek zaměstnavatele uchovávat záznam kamerového systému jen po nezbytně nutnou dobu k naplnění účelu instalace kamer. Z logiky věci vyplývá, že tato zásada se bude týkat pouze kamerových systémů se záznamem. Doba uchování záznamu se může různit ve vazbě na prostor, který kamera snímá nebo i v možnosti přístupu zaměstnavatele k záznamům. Není tedy možné stanovit ideální a jedinou správnou dobu uchování záznamu a je nutné posoudit dobu uchování záznamu u každé kamery jednotlivě.[79]

Metodika přesto stanovuje jako maximální, pro většinu případů dostačující, dobu uchování 72 hodin. Pokud by tato doba měla být překročena, je zaměstnavatel povinen řádně zdůvodnit nezbytnost tohoto prodloužení.[80]

Nutnost odlišných dob uchování záznamu můžeme přiblížit příkladem obchodu s exklusivním oblečením. U kamery, jež monitoruje prostor u pokladny za účelem ochrany majetku, a to především přijatých peněz je dostačující doba 24 hodin. Každý večer se totiž kasa uzavírá a přijaté peníze se počítají. Pokud by

[77] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-02]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.
[78] Tamtéž.
[79] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 204.
[80] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-02]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

určitá částka chyběla, zaměstnavatel může použít kamerový záznam ke kontrole, zda nedošlo k odcizení peněžní částky zaměstnancem, přičemž se záznam poté může stát důkazním materiálem pro orgány činné v trestním řízení. Prostor prodejny je poté sledován několika kamerami, které mají za cíl ochránit především zboží obchodníka. Záznamy z těchto kamer jsou shodně uchovávány po dobu 30 dnů, a to z důvodu pravidelné kompletní inventury zboží právě po této době. Oblast vchodu do prodejny je poté střežena jednou kamerou, která uchovává záznam po dobu 72 hodin. Vzhledem k tomu, že obchod není nikdy zavřený déle než po tuto dobu, obchodníkovi tato doba postačí ke zjištění, že došlo k vloupání do prodejny.[81]

Na závěr je nutné podotknout, že pokud dojde k užití záznamu pro účely trestního či přestupkového řízení, nezapočítává se doba uchování záznamů takovýchto mimořádných událostí. Záznam je uchován až do vyřízení věci a až poté může být smazán.[82]

4.1.6 Zásada zabezpečení údajů

Zásada bezpečnosti údajů v sobě skrývá zásadu integrity, důvěrnosti a odpovědnosti zaměstnavatele. Zakotvuje povinnost zaměstnavatele přijmout taková technická a organizační opatření, která zajistí ochranu získaných osobních údajů před neoprávněným zpracováním nebo před případným zničením či jiným poškozením záznamů. Součástí zásady je i ochrana dat před přístupem neoprávněné osoby.

Zásada odpovědnosti souvisí s proaktivním přístupem zaměstnavatele, který musí být schopen ÚOOÚ řádně prokázat, že zpracování osobních údajů probíhá v souladu s GDPR a že zaměstnavatel přijal opatření, která zabrání porušení GDPR.[83]

---

[81] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 206.

[82] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-02]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

[83] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7. s. 39.

4.2 Právní základ pro zpracování osobních údajů kamerovými systémy

Zpracování osobních údajů je bez výjimky vždy podmíněno existencí právního titulu. Pokud by totiž došlo ke zpracování osobních údajů bez platného právního základu, bylo by toto jednání od počátku nezákonné. Každý právní titul pro zpracování osobních údajů je spojen s konkrétním účelem tohoto zpracování.

Právní důvody jsou vypočteny v článku 6 odst. 1 GDPR, pro zvláštní kategorii citlivých údajů poté v článku 9 odst. 2 GDPR.[84]

Dle článku 6 odst. 1 se jedná o souhlas subjektu údajů, plnění smlouvy jejíž je subjekt údajů smluvní stranou, plnění právní povinnosti uložené zákonem, životně důležité zájmy, plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, na základě oprávněného zájmu správce[85] nebo třetí osoby.[86]

Avšak pro problematiku kamerových systémů na pracovišti je významný pouze právní titul oprávněného zájmu správce nebo třetí osoby, tedy zaměstnavatele, souhlasu zaměstnance a zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu. Pro účely této práce budou podrobněji popsány pouze první dva tyto právní tituly.

4.2.1 Oprávněný zájem zaměstnavatele

Oprávněný zájem zaměstnavatele je ÚOOÚ preferovaným právním základem ke zpracování osobních údajů kamerovými systémy[87], a to především pokud je zaměstnavatelem soukromý subjekt.[88] Dle Morávka má tento právní titul pro zpracování osobních údajů *de facto* shodné důsledky jako vnitrostátně zakotvený „*závažný důvod spočívající ve zvláštní činnosti zaměstnavatele*“, který

[84] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 194.
[85] Pojmem správce se dle GDPR rozumí osoba (fyzická či právnická), jež individuálně nebo společně s jinými určuje účel a prostředky zpracování a je za toto zodpovědný.
[86] Článek 6 odst. 1 GDPR.
[87] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-05]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.
[88] 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. s.345.

dle § 316 odst. 2 zákoníku práce opravňuje zaměstnavatele ke kontrole a sledování zaměstnance na pracovišti.[89]

Pro široký výklad toho, co oprávněným zájmem může být, je třeba důsledného posouzení, zda zájmy zaměstnavatele převažují zájmy a základní práva a svobody zaměstnance. Toto posouzení je zaměstnavatel povinen provést před samotným zavedením kamerových systémů na pracovišti formou tzv. balančního testu, který musí ÚOOÚ kdykoliv doložit.[90] Balančnímu testu se dále budu podrobněji věnovat v kapitole 4.4.1.

Mezi nejčastější zájmy opravňující zaměstnavatele k instalaci kamerových systémů patří ochrana majetku zaměstnavatele a zdraví a bezpečnosti při práci zaměstnance.

4.2.2 Souhlas zaměstnance

Tento právní titul byl využíván v českém právním řádu zaměstnavateli v předchozí praxi velice hojně. Důvodem toho byla zřejmě ne úplně správná formulace v zákoně o ochraně osobních údajů. Ten souhlas subjektů údajů formuloval souhlas jako primární právní titul ke zpracování osobních údajů a zbylé tituly (jako byly například zpracování nezbytné pro plnění právní povinnosti nebo pro ochranu oprávněného zájmu správce) postavil na úroveň výjimek z udělení souhlasu.

S účinností GDPR začal i ÚOOÚ pracovat s variantou, že souhlas je pouze jedním z možných právních titulů, které stojí na stejné úrovni jako jiné právní tituly GDPR definované. Na toto reagovala i nově zavedená Metodika ÚOOÚ, která zaměstnavatelům a všem správcům kamerových systémů tento právní titul pro zavedení kamerového systému výrazně nedoporučuje.[91]

Nevýhoda tohoto právního základu pro sledování zaměstnanců na pracovišti spočívá především v jeho vrtkavosti. Souhlas totiž může subjekt údajů, zaměstnanec, kdykoliv odvolat a zaměstnavatel bude muset neprodleně kamerové systémy pozastavit, omezit či snad úplně vypnout. ÚOOÚ proto kamerové

[89] MORÁVEK, Jakub. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. Právní rozhledy, 2017, č. 17, s. 573-581.
[90] 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. s.345.
[91] NONNEMANN, František. Nová metodika ÚOOÚ ke kamerám: Jste v souladu? GDPR.cz [online]. 2014 [cit. 2024-03-05]. Dostupné z: https://www.gdpr.cz/nova-metodika-uoou-ke-kameram-jste-v-souladu.

sledování na základě titulu souhlasu stanovuje jen jako určitou alternativu a poslední možnost zákonného monitoringu pomocí kamerového systému, za předpokladu, že nelze aplikovat právní titul jiný a zároveň je kumulativně splněna podmínka možnosti vymezení monitorovaných osob.

Avšak znovu musíme zmínit, že Metodika je právně nezávazným dokumentem, takže pokud by se zaměstnavatel přeci jen rozhodl instalovat kamerový systém na základě právního titulu souhlasu, i přes nedoporučení ÚOOÚ, je povinen splnit následující podmínky.

Udělený souhlas zaměstnavateli musí být svobodným, vědomým a informovaným projevem vůle zaměstnance, který má zaměstnavatel povinnost doložit po celou dobu kamerového sledování. Splnění přívlastku svobodný může být ale velice problematický a diskutabilní. To zejména s přihlédnutím k nerovnovážnému postavení, které mezi sebou zaměstnanec a zaměstnavatel mají, obzvlášť pokud by v postavení zaměstnavatele stál orgán veřejné moci. Pro naplnění svobodného souhlasu zde tedy nesmí existovat riziko zastrašování nebo negativních důsledků neudělení souhlasu.

Zaměstnanec dále musí být zaměstnavatelem informován o zpracovávání osobních údajů za pomocí kamerových systému nejpozději při udělení tohoto souhlasu.

V situaci, kdy by zaměstnavatel výrazným způsobem upravoval kamerový systém, čímž se má namysli především prodloužení doby uchování záznamu, rozšíření monitorovaných prostorů či například změnu režimu kamerového systému bez záznamu na kamerový systém záznamový, musí dojít k zajištění nového souhlasu zaměstnance.

V neposlední řadě musí mít zaměstnavatel upraveny postupy pro případ, kdy současný zaměstnanec souhlas odvolá či neudělí souhlas opětovně po zavedení změny v monitoringu a též pro případ nově nastupujícího zaměstnance, který souhlas takovýto souhlas neudělil.[92]

[92] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-16]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

4.3 Zajištění práv subjektů údajů

Zaměstnanec jako subjekt údajů se nachází oproti zaměstnavateli jako správci v nerovném a znevýhodněném postavení. GDPR si proto klade za cíl vyrovnání tohoto mocenského vztahu. Z tohoto důvodu jsou tato práva zakotvena v kapitole III GDPR a představují jeden z klíčových prvků ochrany osobních údajů v členských státech EU.

V následujících kapitolách této diplomové práce se proto budeme věnovat jednotlivým právům.

4.3.1 Informační povinnost

Informační povinnost je nejdůležitějším faktorem pro naplnění zásady transparentnosti stanovené v článku 13 GDPR, protože je předpokladem pro uplatnění dalších práv subjektů údajů spojených se zpracováním osobních údajů za pomocí kamerového systému. Zaměstnavatel nese odpovědnost za přijetí dostatečných opatření, která umožní zaměstnancům řádně a včas uplatnit jejich náležící práva.

V případě kamerových systémů je vhodné využít metodu vrstvení informací, tedy nejdříve informovat subjekty údajů na základní úrovni bez větších podrobností a poté umožnit subjektu získání podrobnějších informací.[93]

4.3.1.1 První vrstva informační povinnosti zaměstnavatele

Jak již bylo v předchozí kapitole řečeno, první vrstva informační vrstvy slouží především k obecnému seznámení fyzické osoby vstupující do monitorovaného prostoru, a to ať už se jedná o zaměstnance či jinou osobu vstupující na pracoviště. Mezi tyto obecné informace řadíme identifikaci včetně kontaktu na provozovatele kamer, účel a právní základ zpracování kamerového sledování, poučení subjektu údajů o jejich právech a v neposlední řadě také odkaz na druhou vrstvu informací,[94] přičemž odkazu na druhou vrstvu informací bude věnována podrobněji pozornost v následující kapitole.

---

[93] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 237.

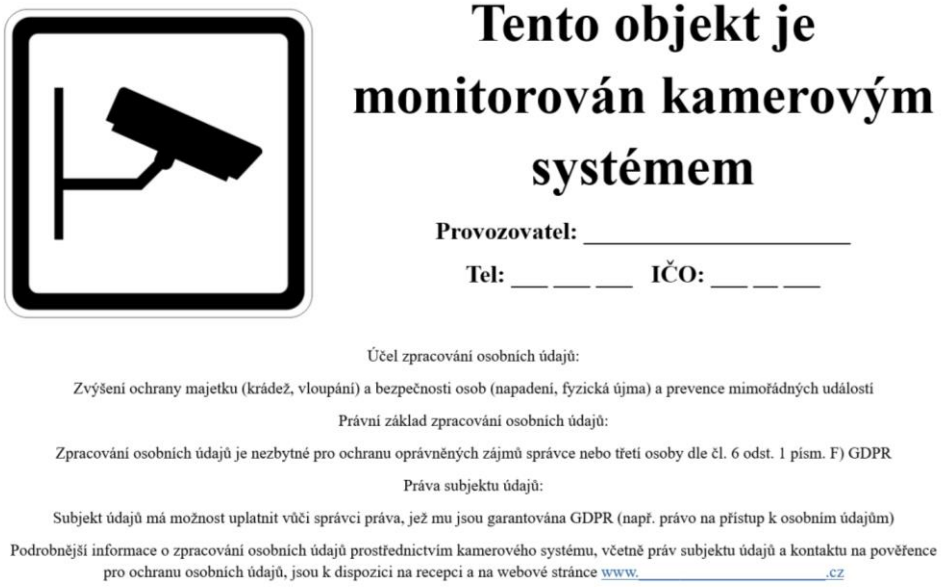
[94] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-16]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

Pro realizaci této první vrstvy je Metodikou i Pokyny 3/2019 doporučeno využití grafického znázornění kamerového systému, tedy piktogramu kamery na informační tabulce.[95] Tato informační tabulka by měla být umístěna tak, aby každá fyzická osoba vstupující do prostoru, který střeží kamerový systém byla s tímto seznámena ještě před vstupem do tohoto prostoru, tedy předtím, než má kamera možnost takovou osobu identifikovat[96]. Na příklad, pokud by byl monitorován sklad, jenž by byl přístupný dvěma vchody – z šatny pro pracovníky a vstupem pro zákazníky z prodejny, která by střežena nebyla, musí být na oba tyto vchody zhruba ve výšce očí označeny právě touto informační tabulkou.

Informační tabulka není formálně standardizována, je ale nutné, aby se na ní krom piktogramu kamery objevil též nápis upozorňující na to, že je daná oblast monitorována kamerovým systémem, to ve velikosti písma, která umožňuje čitelnost i z větší vzdálenosti.[97]

Zaměstnavatel by také neměl zapomenout vzít při realizaci první vrstvy v potaz složení jeho zaměstnanecké základny. V případě, že by pro něj vykonávali práci slabozrací či nevidomí lidé, je nutné první vrstvu podřídit i jim. Z tohoto důvodu je tedy vhodné, aby byla informační tabulka nahrazena alternativou v podobě zvukového oznámení.[98] To by se ovšem nemělo dle mého názoru ozvat až při otevření dveří do monitorované oblasti, protože v tu chvíli už by bylo možné osobu identifikovat, třebaže by vzápětí dané dveře zavřela. Z tohoto důvodu bych doporučila umístit čidlo spínající zvukové oznámení při pohybu osoby ještě před dané dveře vedoucí do monitorované oblasti. Rovněž by měl zaměstnavatel zohlednit jazykovou vybavenost svých zaměstnanců a případných zákazníků nebo jiných osob pravidelně se vyskytujících v monitorovaném prostoru pracoviště a vedle česky psaných informačních tabulek umístit i ty cizojazyčné.

[95] Návrh informační tabulky níže v textu.
[96] Tamtéž.
[97] Tamtéž.
[98] Tamtéž.



Tento objekt je monitorován kamerovým systémem

Provozovatel: _____

Tel: ___ ___ ___ **IČO:** ___ ___ ___

Účel zpracování osobních údajů:

Zvýšení ochrany majetku (krádež, vloupání) a bezpečnosti osob (napadení, fyzická újma) a prevence mimořádných událostí

Právní základ zpracování osobních údajů:

Zpracování osobních údajů je nezbytné pro ochranu oprávněných zájmů správce nebo třetí osoby dle čl. 6 odst. 1 písm. F) GDPR

Práva subjektu údajů:

Subjekt údajů má možnost uplatnit vůči správci práva, jež mu jsou garantována GDPR (např. právo na přístup k osobním údajům)

Podrobnější informace o zpracování osobních údajů prostřednictvím kamerového systému, včetně práv subjektu údajů a kontaktu na pověřence pro ochranu osobních údajů, jsou k dispozici na recepci a na webové stránce www._____.cz

Návrh informační tabulky[99]

4.3.1.2 Druhá vrstva informační povinnosti zaměstnavatele

Druhá vrstva informací se vyznačuje podrobným popisem veškerých informací, v souvislosti s kamerovým sledováním, které musí být uvedeny obecně již v první vrstvě. Dále je druhá vrstva rozšířena například o informaci o režimu fungování kamer, jejich počtu a o podrobný popis práv subjektu údajů.

Pro odkaz na druhou vrstvu je velmi často v první vrstvě využíván QR kód[100] odkazující na webové stránky poskytující podrobné informace. Informace v druhé vrstvě by však měly být alternativně zpřístupněny i v tištěné verzi. Pokud by si vybral správce kamerového systému jednu či druhou verzi bez možnosti alternativy mohlo by to být velice problematické. Správce je totiž povinen umožnit osobě vstupující do monitorované oblasti umožnit získání těchto informací i bez nutnosti vstupu do této střežené oblasti. V tohoto důvodu je vhodné, aby podrobné informace, které jsou dostupné v tištěné formě na

[99] BURIAN, David. ÚOOÚ. Seminář k metodice návrhu a provozování kamerových systémů [online]. 2024. s. 20 [cit. 2024-03-19]. Dostupné z: https://uoou.gov.cz/media/seminare-uoou/prezentace/2024-03-06-seminar-uoou-metodika-ke-kameram.pdf.

[100] QR kód z anglického quick response code je čtvercový obrazec, který podobně jako klasický čárový kód, v sobě nese data.

informační přepážce nebo recepci při vstupu do budovy byly zveřejněné na i webu či dostupné na telefonní lince a naopak.[101]

Za dostatečné splnění informační povinnosti v druhé vlně nelze dle Morávka považovat stav, kdy by měly být informace ústně sděleny subjektu obsluhou v maloobchodě[102] dle mého stejně i na recepci jakéhokoliv pracoviště, pokud by k tomuto nebyl tento zaměstnanec speciálně proškolen. Zaměstnavatel jako správce má povinnost, dle zásady odpovědnosti, dozorujícímu úřadu prokázat splnění informační povinnosti. Z tohoto důvodu je tedy vhodné přiklonit se k formálnější variantě v podobě psaného textu.[103]

Informace o kamerovém systému ve druhé vrstvě by měly zahrnovat informaci o účelu a rozsahu zpracování osobních údajů, identifikaci zaměstnavatele jako správce pomocí názvu, IČO[104] a sídla. Případně též identifikaci pověřence pro ochranu osobních údajů, pokud je taková pozice v rámci společnosti zřízena, zde postačí jméno, příjmení, telefonní číslo nebo e-mailová adresa. Dále též právní základ a adresu místa pro zpracování osobních údajů, informaci o příjemci nebo kategorii příjemců, kterým jsou osobní údaje zpřístupněny a též informaci o předávání osobních údajů do třetích zemích. V neposlední řadě by zde měl být uveden též počet kamer, režim jejich fungování, informace o automatizovaném rozhodování včetně profilování a poučení práv subjektů o jejich právech vůči správci. [105]

4.3.1.3 Informační povinnost zaměstnavatele dle zákoníku práce

Obdobně jako GDPR stanovuje informační povinnost obecně pro všechny správce osobních údajů na evropské úrovni, stanovuje zákoník práce v poměru speciality k GDPR informační povinnost pro zaměstnavatele v České republice, to konktrétně v § 316, odst. 3, tedy „*jestliže je u zaměstnavatele dán závažný důvod*

[101] EUROPEAN DATA PROTECTION BOARD. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky [online]. 2020. s. 7-8. [cit. 2024-03-16]. Dostupné z: https://edpb.europa.eu/edpb_guidelines_video_devices_cs.pdf.
[102] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 238.
[103] Tamtéž.
[104] Osmimístné identifikační číslo osoby sloužící v České republice k identifikaci právnické osoby, podnikající fyzické osoby či organizační složky státu.
[105] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-21. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

spočívající ve zvláštní povaze jeho činnosti, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.“[106]

V případě otevřené kontroly pomocí kamerových systémů je zaměstnavatel povinen splnit svou informační povinnost ještě před začátkem monitoringu[107] stejně jako tomu je dle GDPR. Pokud jde o skrytou kontrolu, musí zaměstnavatel splnit informační povinnost v plném rozsahu ihned po jejím ukončení. Obecně by měl zaměstnavatel předem alespoň obecně oznámit možnost kontroly, což se samozřejmě týká všech možných druhů kontroly dle druhého odstavce.[108]

Před instalací kamerového systému na pracovišti má zaměstnavatel dle zákoníku práce povinnost informovat zaměstnance o několika klíčových aspektech. Především musí zaměstnavatel sdělit rozsah kontroly a dobu, po kterou bude kontrola probíhat. V rámci definice rozsahu dle Morávka by měl zaměstnavatel specifikovat, které pracovní úkony budou sledovány, a identifikovat místa, kde budou kamery umístěny.

Zákoník práce přitom dále neupravuje, jakou formou má zaměstnavatel informační povinnost splnit. Je tedy možné ji splnit i pouhou ústní formou. Pro zajištění souladu se zákoníkem práce a GDPR, pro kontrolní účely úřadu inspekce práce nebo ÚOOÚ, nebo případné soudní spory se zaměstnanci, je ale vhodné zaměstnavateli doporučit, aby informační povinnost splnil písemnou formou. Tato forma, na rozdíl od té ústní, zaručuje stvrzení o tom, že zaměstnanci byly informace o kamerovém sledování předány. Zákoník práce přitom požaduje přímost tohoto předání. V přímosti předání informace je podle Morávka spatřováno adresné předání informace zaměstnanci, tedy poskytnutí této informace prostřednictvím kanálu, se kterým se zaměstnanec má povinnost seznámit.[109] Z mého pohledu je proto nejvhodnější cestou předání informace zaměstnanci řádně přijatý a vyhlášený interní předpis, z tohoto důvodu mu bude věnována kapitola 5.4.2. této diplomové práce.

---

[106] § 316, odst. 3 zákoníku práce

[107] Toto není zákoníkem práce explicitně stanoveno, avšak nutnost předchozího oznámení monitoringu dovozujeme z judikatury NSS, konkrétně z rozsudku sp. zn. 5 As 158/2012.

[108] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 384.

[109] Tamtéž.

4.3.2 Právo na přístup k osobním údajům

Právo na přístup k osobním údajům je na rozdíl od výše popsaného práva na informace právem aktivním, což znamená, že přístup ke zpracovávaným osobním údajům zaměstnavatel umožní pouze subjektu, jež o to požádal.

Dle GDPR má toto právo dvě roviny. Dle té první má jednotlivec právo, na základě své žádosti, získat od potenciálního správce potvrzení o zpracování či nezpracování jeho osobních údajů. Při kladném potvrzení o zpracování osobních údajů v této první rovině, má subjekt údajů v druhé rovině též právo na přístup k těmto informacím.[110]

Právo na přístup k osobním údajům, na rozdíl od předchozí právní úpravy v podobě zákona o ochraně osobních údajů, dnes již jasně zahrnuje také právo subjektu na poskytnutí kopie zpracovávaných údajů, tedy v případě kamerového systému právo na poskytnutí předmětného záznamu.[111]

V kontextu kamerových systémů je však nutné odlišit, zda je pořizován záznam či nikoliv. V situaci, kdy zaměstnavatel monitoruje pracoviště pouze pomocí kamerového systému bez záznamu, může, na základě žádosti, poskytnout subjektu pouze omezenou informaci v první rovině, tedy že momentálně se žádné jeho osobní údaje již nezpracovávají. Pokud by však zaměstnavatel jako správce osobních údajů měl kamerový záznam k dispozici, je jeho povinností oprávněné osobě zajistit přístup k tomuto záznamu a oprávněná osoba může svého práva na přístup k osobním údajům využít naplno.[112]

Oprávněnou osobou nemusí být ale pouze subjekt údajů. O kopii kamerového záznamu může požádat i ten zaměstnanec, který se zrovna na kamerovém záznamu neobjevuje. Zaměstnavatel mu kopii kamerového záznamu vydá za předpokladu, že všechny ostatní osoby nacházející se na monitorovaném pracovišti k tomuto udělí souhlas. Rovněž je zaměstnavatel povinen poskytnout kamerový záznam orgánům činným v trestním řízení nebo pojišťovnám v případě pojistné události.

---

[110] Článek 15 GDPR.
[111] ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Praha: Leges, 2019. Teoretik. ISBN 978-80-7502-373-5. s. 150.
[112] EUROPEAN DATA PROTECTION BOARD. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky [online]. 2020 [cit. 2024-03-22]. Dostupné z: https://edpb.europa.eu/edpb_guidelines__video_devices_cs.pdf.

Problematickou se stává situace, kdy se spolu s osobou žádající o přístup k záznamu objeví v záznamu ještě další identifikovatelná osoba. Zaměstnavatel stále musí oprávněné osobě umožnit přístup ke zpracovaným údajům, zároveň je ale povinen před předáním záznamu další identifikovatelnou osobu, za předpokladu, že neudělila souhlas s poskytnutím kopie, učinit neidentifikovatelnou, jinak by mohla být nepříznivě dotčena její práva. Anonymizace osoby zaměstnavatel dosáhne za pomocí technických prostředků jako je rozostření nebo maskování.[113]

Oprávněný subjekt má nárok na bezplatné poskytnutí jedné kopie svých osobních údajů. Pokud zaměstnanec požaduje více kopií ve fyzické podobě, může zaměstnavatel jako správce údajů vyžadovat úhradu nákladů spojených s jejich vytvořením. V případě, že je žádost zjevně nedůvodná nebo nepřiměřená, může správce údajů požadovat přiměřený poplatek.

Zaměstnavatel má také právo odmítnout vyhovět žádosti o poskytnutí kopie, pokud je žádost opakovaná nebo zjevně nedůvodná. Toto opatření bylo zavedeno zákonodárcem s cílem zabránit potenciálně šikanóznímu chování zaměstnanců, kteří by mohli zneužívat svá práva na přístup k osobním údajům k vytváření tlaku na svého zaměstnavatele.[114]

4.3.3 Právo na opravu osobních údajů

Právo na opravu je projevem zásady přesnosti zpracovávaných osobních údajů. Ve vztahu ke zpracování osobních údajů kamerovými systémy je toto právo jen omezeně uplatnitelné na kamerové systémy uchovávající záznam. Vzhledem k povaze videozáznamu, který představuje autentické zachycení reality, je téměř nemožné provést zpracování nepravdivých nebo jinak nepřesných osobních údajů.

Jediným možným způsobem opravy kamerového záznamu by mohlo být vytvoření dokumentace a evidence rozdílu mezi reálným a strojovým časem.[115]

---

[113] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-21. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

[114] Článek 12, odst. 5 GDPR

[115] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-23. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

4.3.4 Právo na výmaz

Právo na výmaz, které je v široké veřejnosti známé též jako právo na to být zapomenut, je jedním ze základních práv subjektu údajů, které je zakotveno v článku 17 GDPR. Toto právo vychází ze zásad minimalizace dat a omezení doby jejich uchování. Ačkoliv bylo veřejnosti často prezentované jako novinka a vlastně i hlavní motiv pro vznik GDPR, toto právo bylo upraveno již v předchozí právní úpravě. Rozdíl spočívá v tom, že GDPR tento institut blíže specifikuje.[116]

Podobně jako právo na opravu osobních údajů, právo na výmaz v kontextu kamerových systémů je aplikovatelné pouze v případě, že zpracování osobních údajů subjektu přesahuje rámec monitoringu v reálném čase. Jinými slovy, toto právo je uplatnitelné pouze v situaci, kdy je kamerový systém vybaven funkcí záznamu.[117]

Právo na výmaz je aktivním právem subjektu údajů, avšak není právem absolutním. Zaměstnavatel, v roli správce osobních údajů, má povinnost provést výmaz kamerového záznamu bez zbytečného odkladu, ale pouze za předpokladu, že je naplněna některá z následujících taxativně vymezených podmínek. Mezi tyto podmínky řadíme: nepotřebnost záznamu pro naplnění původního účelu monitoringu, odvolání souhlasu subjektu s kamerovým sledováním bez současné existence jiného právního důvodu pro monitoring, protiprávnost kamerového sledování a též má povinnost výmazu v případě, pokud bude subjektem vznesena námitka, jež bude věcně vyhodnocena jako důvodná.[118]

To že se nejedná o právo absolutní dokazuje i množství výjimek při kterých se toto právo vůbec neuplatní. Výjimkami jsou situace, kdy je uchování záznamu nezbytné pro splnění právní povinnosti, z důvodu veřejného zájmu v oblasti veřejného zdraví nebo archivace, pro určení, výkonu nebo obhajobu právních nároků a také jako pro výkon práva na svobodu projevu.[119]

Na závěr je třeba podotknout, že zaměstnavatel nemusí provést úplné vymazání záznamu, aby dosáhl souladu s GDPR. Výmaz osobních údajů lze

---

[116] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 247.
[117] EUROPEAN DATA PROTECTION BOARD. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky [online]. 2020. s. 23-24. [cit. 2024-03-24]. Dostupné z: https://edpb.europa.eu/edpb_guidelines__video_devices_cs.pdf.
[118] Tamtéž.
[119] Článek 17, odst. 3 GDPR

realizovat pomocí technologických prostředků, jako je rozostření nebo maskování identifikovatelné osoby, která o to požádala. Bez ohledu na způsob provedení výmazu osobních údajů by měl zaměstnavatel vyhotovit protokol o tomto procesu. Protokol by měl obsahovat identifikaci žadatele a osoby, která výmaz provedla. Dále by měl být identifikován vymazaný nebo jinak upravený záznam. A konečně, protokol by měl obsahovat datum provedení výmazu.[120]

4.3.5 Právo na omezení zpracování

Právo na omezení zpracování, jak je stanoveno v GDPR, představuje sekundární nástroj pro subjekty údajů, který by měl být automaticky aktivován zaměstnavatelem jako správcem údajů ve chvíli, kdy subjekt požádal o výmaz záznamu, subjektem byla vznesena námitka nebo za situace, kdy subjekt požaduje opravu zpracovaných osobních údajů. Jenom prostřednictvím automatického uplatnění tohoto práva bez žádosti zaměstnance je totiž možné dosáhnout souladu se zásadami zákonnosti a minimalizace údajů. Přičemž sekundárnost tohoto nástroje spojená s jeho sporadickou využitelností subjekty spočívá zejména v jeho dočasné povaze.[121]

Subjekt údajů má také možnost samostatně požádat o omezení zpracování, pokud zaměstnavatel automaticky neaplikuje omezení v případech, které byly výše uvedeny. Tato možnost je také dostupná, pokud subjekt údajů má za to, že zpracování jeho osobních údajů je v rozporu s právem a namísto výmazu osobních údajů (záznamu) preferuje omezení jejich použití. Stejně tak, pokud zaměstnavatel již nepotřebuje záznam pro účel, pro který byl pořízen, ale zaměstnanec požaduje tento záznam pro určení, obhajobu nebo výkon právních nároků.[122]

Jedním z typických příkladů využití práva na omezení zpracování v kontextu pracovního práva je situace, kdy dojde k úrazu zaměstnance na monitorovaném pracovišti. Pokud má tento zaměstnanec sjednané úrazové pojištění, může mu kamerový záznam posloužit jako důkaz pro doložení škodní události pojišťovně. Z tohoto důvodu zaměstnanec podá zaměstnavateli žádost,

[120] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024. s. 21. [cit. 2024-03-23. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.
[121] ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Praha: Leges, 2019. Teoretik. ISBN 978-80-7502-373-5., s. 155-156.
[122] Článek 18, odst. 1 GDPR

aby uchoval konkrétní záznam dokumentující vznik úrazu, čímž dojde k omezení zpracování, až doby, kdy bude tento záznam poskytnut zaměstnanci pro účely obhajoby jeho nároku vůči pojišťovně.[123]

4.3.6 Právo na přenositelnost údajů

Právo na přenositelnost údajů je opravdu jedinou novinkou, kterou nám GDPR přineslo, avšak v kontextu kamerových systémů právo na přenositelnost údajů pro subjekt údajů nenabízí praktickou hodnotu. Toto je řešeno v rámci práva subjektu údajů na přístup k osobním údajům, kdy má subjekt údajů právo získat kamerové záznamy týkající se jeho osoby.[124]

4.3.7 Právo vznést námitku proti zpracování

GDPR přiznává zaměstnanci či sledovaném subjektu právo na vznesení námitky proti tomuto sledování, především pokud je založeno na právním důvodu oprávněného zájmu zaměstnavatele.[125] Tuto námitku může zaměstnanec vznést kdykoliv v průběhu sledování avšak námitka jako taková by měla být odůvodněna konkrétní situací, která v zaměstnanci vyvolala dojem, že kamerové sledování zasahuje do jeho práva na soukromí.

V akademických kruzích probíhá debata o procesu, který následuje po vznesení námitky. Dle Nulíčka je nutné po obdržení námitky bez zbytečného odkladu okamžitě přestat osobní údaje osoby, jež námitku vznesla, zpracovávat. Nebo alespoň zpracování omezit do doby, než bude námitka posouzena jako odůvodněná. Po posouzení odůvodněnosti, před závěrečným věcným posouzením námitky, by se měl zaměstnavatel zdržet zpracování nad míru sloužící účelu určení, výkonu nebo obhajoby právních nároků.[126] Naopak Uřičař nebo Zahradníček zastávají názor, že ukončení zpracování osobních údajů musí zaměstnavatel učinit až za situace, pokud neprokáže svůj oprávněný zájem

[123] ŽŮREK, Jiří. GDPR v personalistice. Olomouc: ANAG, [2019]. Práce, mzdy, pojištění. ISBN 978-80-7554-210-6. s. 81.
[124] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024. s. 22. [cit. 2024-03-23. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.
[125] Dalším právním důvodem pro vznesení námitky je též kamerové sledování nezbytné pro splnění úkolu prováděného ve veřejném zájmu, avšak pro minimální využitelnost v kontextu diplomové práce se dále tímto právním důvodem nebudeme zabývat.
[126] NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3. s.229.

zajišťující možnost zásahu do práv a svobod zaměstnanců.[127] K tomuto výsledku posouzení musí dojít zaměstnavatel nejpozději ve lhůtě jednoho měsíce od obdržení námitky.

Pro prokázání oprávněného zájmu zaměstnavatele je považováno za nedostatečné pouhé odkázání na výsledek původního balanční testu vedoucího k instalaci kamerových systémů na pracovišti. Aby tedy zaměstnavatel unesl důkazní břemeno, je nutné vyhotovit nový balanční test v kontextu podané námitky s opravdu přesvědčivým odůvodněním převažujících zájmů zaměstnavatele.

Pokud zaměstnavatel důkazní břemeno neunese, vzniká zaměstnanci jako subjektu údajů též právo na výmaz, které je blíže rozebráno v kapitole 4.3.4.

4.3.8 Kontrolní oprávnění zaměstnavatele dle zákoníku práce

Zaměstnavatel je oprávněn vykonávat kontrolu nad svými zaměstnanci na základě § 316 zákoníku práce. Dle Nonnemanna je kontrolu podle předmětného paragrafu třeba chápat spíše jako kontinuální dohled nad zaměstnancem, přičemž toto usuzuje z terminologie použité zákonodárcem.[128] Shodný názor má i Morávek, který v tomto kontextu definuje sledování jako opakované systematické kontrolování zaměstnance prostřednictvím kamerového systému.[129]

Kamerový systém jako prostředek kontroly nad zaměstnanci může zaměstnavatel využít z titulu druhého odstavce výše zmíněného paragrafu. Ačkoliv zákoník práce explicitně použití kamerového systému jako nástroje pro monitoring zaměstnanců nestanovuje, na rozdíl od odposlechu nebo záznamu telefonických hovorů, lze tento nástroj zařadit pod pojem sledování, který nebyl zákonodárcem blíže definován. Tento ať už skrytý či nedbalostí záměr zákonodárce otevírá širší prostor pro aplikaci nových kontrolních mechanismů, jako jsou právě kamerové systémy, v rámci pracovního práva.

---

[127] 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. s.345.
ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Praha: Leges, 2019. Teoretik. ISBN 978-80-7502-373-5. s. 154.

[128] NONNEMANN, František: Soukromí na pracovišti, Právní rozhledy. Č. 7/2015, s. 229.

[129] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 377.

Podle ustanovení zákoníku práce je pro zavedení kamerového systému na pracovišti nezbytné splnit dvě kumulativní podmínky. První podmínkou je existence závažného důvodu, který je odvozen od specifické povahy činnosti zaměstnavatele a tou druhou podmínkou je splnění informační povinnosti vůči zaměstnanci. Informační povinnosti dle zákoníku práce byla věnována kapitola 4.3.1.3 této práce.

Jak již bylo řečeno v kapitole 4.2.1., existence závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele se ve skutečnosti shoduje s právním titulem oprávněného zájmu dle GDPR.[130] Zákonodárce tento pojem opět nijak nedefinuje, a tak se zde vytvořen velký prostor pro interpretaci.

Podle Štefka je nemyslitelné, aby se tento pojem vztahoval pouze na zvláště nebezpečné pracoviště jako je například jaderná elektrárna. Monitoring má být umožněn na základě důvodů jakými jsou ochrana zdraví a bezpečnosti zaměstnance a ochrana majetku [131]

Morávek se drží neurčitého tónu zákonodárce i když na rozdíl od Štefka blíže přibližuje pojem „*závažný důvod*“ a uvádí, že oprávněnost monitoringu na pracovišti by měla být specificky posouzena případ od případu na základě testu přiměřenosti.[132]

Do třetice dle názoru Nonnemanna musí být pro zavedení monitoringu na pracovišti předmět činnosti zaměstnavatele v určitém směru specifický.[133]

Dle mého názoru vycházejícího z praxe zaměstnavatelů a výše uvedených názorů má téměř každý zaměstnavatel možnost oprávněného a zákonného monitoringu svých zaměstnanců bez ohledu na předmět jejich činnosti. Avšak před nasazením tak intenzivního prostředku monitoringu, jakým je kamerový systém, bude potřeba důsledného posouzení poměření zájmů zaměstnavatele se zájmy zaměstnance prostřednictvím balančního testu.

---

[130] MORÁVEK, Jakub. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. Právní rozhledy, 2017, č. 17, s. 573-581.
[131] (ŠTEFKO, Martin. § 316 [Majetek zaměstnavatele; soukromí zaměstnance; nesouvisející informace]. In: BĚLINA, Miroslav, DRÁPAL, Ljubomír a kol. Zákoník práce. 4. vydání. Praha: C. H. Beck, 2023, s. 1400, marg. č. 3.)
[132] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 379.
[133] NONEMANN, František. Soukromí na pracovišti. Právní rozhledy. 2015. 3 (7), s. 232.

4.4 Dokumentace potřebná k zavedení kamerového systému na pracovišti

Dokumentace kamerového systému je pro zaměstnavatele důležitá především v kontextu prokázání oprávněnosti zpracování osobních údajů zaměstnanců za pomocí kamerových systémů při možné kontrole ÚOOÚ. Tato dokumentace se skládá ze záznamu o činnostech zpracování, balančního testu, analýzy povinnosti zpracovat DPIA[134] a s tím související případně zpracovaná DPIA, interního předpisu upravující postupy k provozování kamerového systému, doklady o udělení souhlasu se zpracováním osobních údajů, pokud je souhlas právním základem pro zavedení kamerového systému, případnou zpracovatelskou smlouvu a v neposlední řadě též dokumentaci zajišťující informovanost zaměstnanců a dalších osob vstupujících na monitorované pracoviště.

Podrobněji si pro účely této diplomové práce rozebereme a popíšeme balanční test, interní předpis a zpracovatelskou smlouvu.

4.4.1 Balanční test

Balanční test je zvláštním dokumentem, který je zaměstnavatel povinen vypracovat ještě před zavedením kamerového systému na pracoviště, a to v případě, pokud je kamerový sytém instalován na základě právního základu oprávněného zájmu zaměstnavatele, jemuž byla věnována pozornost v kapitole 4.2.1. této diplomové práce. V případě instalace kamerového systému na právním základě souhlasu[135] se názory na nutnost jeho vyhotovení liší, a to dle stanoviska W29 č. 2/2017[136] zejména s ohledem na spornost oprávněnosti a svobodnosti udělení takového souhlasu subjektu údajů v nerovnovážném mocenském vztahu zaměstnanec – zaměstnavatel. ÚOOÚ se z tohoto důvodu od právního titulu souhlasu ke zpracování osobních údajů odvrací, a i když jej lze i nadále využít, nutnost předchozího vyhotovení balančního testu k tomu ÚOOÚ nevyžaduje.[137].

---

[134] DPIA vycházející z anglického Data Protection Impact Assessment znamená posouzení vlivu na ochranu osobních údajů.
[135] Kapitola 5.2.3.
[136] WP29. Stanovisko č. 2/2017 ke zpracování údajů na pracovišti. European Commisson [online]. 2017, S. 4 [cit. 2024-03-18]. Dostupné z: https://ec.europa.eu/newsroom/article29/items/610169.
[137] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024, S. 14. [cit. 2024-03-16]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

Balanční test, označovaný Ústavním soudem též jako test proporcionality je komplexním posouzením, které má za cíl zhodnotit, zda oprávněný zájem zaměstnavatele – jako správce údajů, převyšuje práva subjektu údajů, která jsou chráněna právním řádem na ústavní úrovni.[138]

Tento test vychází ze zásady přiměřenosti, která je v českém právním řádu zakotvena na ústavní úrovni v článku 4 odst. 1 a 4 Listiny základních práv a svobod.[139] Tato zásada je aplikována v situaci, kdy dojde ke kolizi dvou práv a jejím výsledkem by měla být v optimálním případě situace, kdy se z každého práva uplatní v co možná nejvyšší míře maximum. Jejím uplatněním tedy nedochází k situaci, kdy je jedno právo pomyslně vyhraje svou závažností před druhým, nýbrž výsledkem testu je optimalizovat vztah těchto práv tak, aby z nich zůstalo co nejvíce.[140]

Dle stanoviska WP29 č. 6/2014[141] jsou klíčovými faktory pro posouzení ověření vyváženosti:

1) „důležitost oprávněného zájmu zaměstnavatele na monitoringu;
2) nezbytnost a důsledky monitorování pro subjekty údajů;
3) zájmy nebo základní práva svobody subjektu údajů vyžadující ochranu osobních údajů.“[142]

[138] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.
[139] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 33.
[140] WAGNEROVÁ, Eliška. Listina základních práv a svobod: komentář. 2., doplněné a aktualizované vydání. Praha: Wolters Kluwer, 2023. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7676-747-8. S.93.
[141] WP29. Stanovisko č. 6 /2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. European Commisson [online]. 2014 [cit. 2024-03-18]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf.
[142] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

Dle Ústavního soudu ČR je možné omezit základní právo či svobody pouze za situace, kdy takovýto zásah naplní pro dosažení sledovaného cíle následující kritéria:

1) vhodnost – konkrétně zda využití kamerového systému umožňuje zaměstnavateli dosáhnout stanoveného cíle;
2) potřebnost – konkrétně zda neexistuje možnost dosažení cíle zaměstnavatele jinými srovnatelnými prostředky s kamerovým systémem, jež by znamenaly pro zaměstnance menší zásah do jejich práva na soukromí;
3) přiměřenost: konkrétní posouzení toho, zda prospěch dosažený zavedením kamerového systému na pracovišti bude vyšší než narušení soukromí zaměstnance.[143]

Metodikou ÚOOÚ je doporučeno před vyhodnocením těchto třech kritérií, stanovených Ústavním soudem, aby zaměstnavatel zvažující montáž kamerových systémů na pracoviště nejprve popsal tzv. existenci reálného ohrožení. Tuto existenci by měl zaměstnavatel opakovaně posuzovat i po delší době od instalace kamerového systému.

V tomto popisu mají být nastíněny některé mimořádné či pravidelně se opakující situace, které vedly zaměstnavatele právě k instalaci kamerového systému. Mezi tyto situace mohou být zařazeny ty, které se staly přímo na pracovišti, které má být nově monitorováno nebo se statisticky jedná o pracoviště s vyšším mírou bezprostředního nebezpečí. Mezi takové pracoviště se může řadit pošta, klenotnictví nebo také čerpací stanice. V případě, pokud zaměstnavatel prokáže existující reálné ohrožení, přistoupí ke konkrétnímu vyhodnocení jednotlivých kritérií.

Jak už bylo výše řečeno, u kritéria potřebnosti musí zaměstnavatel zvážit, zda by definovaného účelu nešlo dosáhnout i jinými prostředky. Toto provede vytvořením několika variant řešení návrhu kamerového systému a dalších alternativních prostředků, které mají za cíl v co nejmenší možné míře zasáhnout do soukromí jeho zaměstnanců za současného dosažení stanoveného účelu.

[143] MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 33-34.

Jednotlivé varianty poté zaměstnavatel porovná s aktuálním řešením, pokud se již na pracovišti nějaké kamery či obdobná zařízení nacházejí, případně s tzv. nulovým řešením, které dosud žádná opatření k zajištění stanoveného účelu nezahrnuje. [144]

Při návrhu konkrétních variant se zaměstnavatel zaměří na to, zda by bylo možné aplikovat alternativní prostředky pro ochranu majetku zaměstnavatele, ale i pro ochranu zaměstnanců. Mezi takové alternativy patří například vstup na čipy nebo za pomocí přístupových karet. Tato zařízení povolí přístup do speciálních prostor pracoviště pouze vybraným zaměstnancům a zároveň v případě mimořádných událostí má zaměstnavatel přehled o zaměstnancích momentálně se v daném místě pracoviště nacházející. Další alternativou je instalace bezpečnostního alarmu, který by byl schopen detekovat neoprávněný vstup nebo případný pohyb na pracovišti a vyvolat hlasitý poplach.[145]

V jednotlivých variantách navrhujících instalaci kamerových systémů musí zaměstnavatel zvážit počet a umístění jednotlivých kamer, tak aby byl použit pouze minimální počet kamer, a to pouze v nezbytně nutných místech.[146] Při tomto nesmí zaměstnavatel zapomenout, že kamery nelze umisťovat do místností sloužících k odpočinku zaměstnanců, dále do šaten a místností sloužících k výkonu osobní hygieny zaměstnanců, a to ani v případě, pokud by šlo pouze o jejich atrapy.[147] V úvahu by měl vzít zaměstnavatel též nastavení záběru kamer tak, aby byl minimalizován zásah do soukromí zaměstnanců. Úpravu záběru může být realizována natočením samotné kamery, pokud by se tedy jednalo o kamery bez možnosti online ovládání nebo by tato funkce byla u kamery deaktivována. Upravit záběr lze samozřejmě i za pomocí rozostření či celkovým zakrytím části záběru.

---

[144] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-19]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

[145] Jak používat kamery na pracovišti. GEMBALOVÁ, Kristýna. Právní prostor [online]. 2024 [cit. 2024-03-19]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/jak-pouzivat-kamery-na-pracovisti.

[146] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-03-19]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

[147] ÚOOÚ. Přepravní a dopravní společnost (UOOU-04151/20) [online]. 2021 [cit. 2024-03-19]. Dostupné z: https://uoou.gov.cz/cinnost/ochrana-osobnich-udaju/ukoncene-kontroly/kontroly-za-rok-2021/kontrolni-cinnost-v-oblasti-ochrany-osobnich-udaju-2021/prepravni-a-dopravni-spolecnost-uoou-0415120.

Jak již bylo naznačeno výše, minimalizace zásahu do soukromí zaměstnance může být provedena i deaktivováním některých funkcí kamer. Jde především o deaktivaci již zmíněné funkce online pohybu nebo otáčení kamer, dále pořizování audiozáznamu nebo zachycení biometrických dat. V neposlední řadě by měl v jednotlivých variantách zaměstnavatel zvážit též režim kamerového záznamu, tedy zda je nutné monitorovat oblast pracoviště i v pracovní době zaměstnanců nebo je postačující aktivace kamerového systému na základě pohybu na pracovišti či pokynu obsluhy kamerového systému.

Na závěr vybere zaměstnavatel z těchto navržených variantu tu, která se mu zdá pro jeho pracoviště jako nejvýhodnější a podrobí ji dalšímu kritériu, konkrétně kritérium vhodnosti.

Kritérium vhodnosti se zabývá otázkou, zda lze objektivně instalací kamerového systému na pracoviště dosáhnout tíženého účelu. V rámci tohoto kritéria jsou porovnávány finanční náklady na pořízení kamerového systému oproti nefinančním i finančním přínosům instalace, včetně případné návratnosti tohoto řešení. Pokud by v rámci tohoto porovnání vyšly záporné výsledky, měl by zaměstnavatel přistoupit k druhé nejvíce optimální variantě dle předchozího kritéria a tu následně obdobně jako variantu první podrobit kritériu vhodnosti. Takto zaměstnavatel postupuje až do chvíle, nežli nalezne skutečně vhodnou variantu.

Jako poslední krok provede zaměstnavatel posouzení přiměřenosti v užším slova smyslu. To znamená, že variantu, jež se jeví dle předchozího kroku jako skutečně vhodná posoudí z hlediska její přiměřenosti jako zásahu do soukromí zaměstnance. Jestliže by tento zásah nepřevážil zájem správce, je nutné přejít k další vhodné variantě dle prvního kritéria a podrobit ji dalším, nežli je nalezena varianta nejlepší. V rámci tohoto kroku je relevantní provést celkovou analýzu očekávání zaměstnanců, jakožto i analýzu postavení obou stran v rámci pracovněprávního vztahu se zaměřením na zpracování osobních údajů a popisu dodržování základních zásad pro zpracování osobních údajů.[148]

[148] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024. S. 11-14. [cit. 2024-03-19]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.

4.4.2 Interní předpis

Interní nebo také vnitřní předpis je vnitropodnikovým normativním aktem, kterým zaměstnavatel může autoritativně specifikovat práva a povinnosti přiznané zaměstnanci zákoníkem práce. Je důležité poznamenat, že tento interní předpis nesmí v žádném případě ukládat zaměstnanci povinnosti nebo omezovat jeho práva nad rámec toho, co je stanoveno v zákoníku práce. Často se může stát, že tento interní předpis je také předmětem schválení odborového orgánu, který zastupuje zájmy zaměstnanců.

Zaměstnavatel má zájem na tom, aby všechny osoby, které se pravidelně vyskytují na pracovišti, dodržovaly stejná pravidla. Z tohoto důvodu tento předpis zavazuje zaměstnance, a to bez ohledu na to, zda je jeho pracovněprávní vztah založen na právním titulu pracovní smlouvy či dohody o provedení práce nebo dohody o pracovní činnosti.[149] Rovněž se tedy může vztahovat na osoby, jejichž vztah k zaměstnavateli je založen na základě jiného právního vztahu jako je například smlouva o dílo. Toto je důležité pro udržení konzistence a efektivity v pracovním prostředí.

A to i z toho důvodu, že zaměstnavatel má zájem na tom, aby všechny osoby pravidelně se vyskytující na pracovišti dodržovali stejná pravidla.

V případě zavedení kamerového systému na pracovišti se jedná o vnitřní předpis zavádějící organizační opatření vycházející ze vztahu nadřízenosti zaměstnavatele a podřízenosti zaměstnance, proto bývají tyto předpisy označovány jako tzv. akty řízení.[150]

Vnitřní předpis obecně má zaměstnavatel povinnost vydat písemně. To znamená, že v situaci, kdy je vydán vnitřní předpis a jeho účinnost je oznámena pomocí elektronické pošty či intranetu, musí mít zaměstnanec přístup k písemné formě tohoto dokumentu i přes jeho uložení na interním disku zaměstnavatele. K uchování písemné verze a k možnosti nahlédnutí všem zaměstnancům je vnitřní předpis uchován nejlépe na personálním oddělení zaměstnavatele, pokud je takové oddělení zřízeno.

[149] HŮRKA, Petr. Pracovní právo. 5. vydání. Plzeň: Aleš Čeněk, 2023. ISBN 978-80-7380-33-1. s. 78.
[150] BĚLINA, Miroslav. Zákoník práce: komentář. 4. vydání. V Praze: C.H. Beck, 2023. Velké komentáře. ISBN 978-80-7400-951-8. s. 1329.

Dále pro vnitřní předpis obecně platí obligatorní zákaz rozporu se zákoníkem práce a dalšími právními předpisy, porušení tohoto zákazu by mělo za následek neplatnost předpisu, a o buď zcela nebo pouze ve vymezené části. Rovněž je zakázáno vydat vnitřní předpis se zpětnou účinností. Účinnost vnitřního předpisu však může nastat společně s vyhlášením, případně dnem uvedeným ve vnitřním předpisu jako den nabytí účinnosti. Způsob vyhlášení vnitřního předpisu není zákoníkem práce stanoven, zaměstnavatel by proto měl zvolit cestu, která je v rámci pracoviště obvyklá.

Vnitřní předpis bývá vydáván na dobu určitou, zákoník práce poté stanoví jako nejkratší dobu působnosti vnitřního předpisu 1 rok.[151] V praxi se ale velice často setkáme s tím, že jsou vnitřní předpisy upravující postupy v souvislosti se zavedením kamerových systémů na pracovišti vydávány na dobu neurčitou. K tomuto lze dodat, že zákoník práce sice vydání vnitřního předpisu na dobu neurčitou nezakazuje, avšak je nutné, aby byl vnitřní předpis vždy aktualizován spolu se změnou provedenou v kamerovém systému tak, aby i nadále splňoval podmínky stanovené pro ochranu osobních údajů stanovené GDPR a zaměstnavatel byl toto schopen doložit.

Interním předpisem zaměstnavatel zavádí vhodná organizační a technická opatření dle standardů vyžadovaných GDPR a zákonem o zpracování osobních údajů. Pro zaměstnance tento předpis může sloužit jako druhá vrstva informační povinnosti. Takový vnitřní předpis by proto měl obsahovat všechny informace, které tato druhá vrstva musí obsahovat, což je uvedeno výše v textu kapitoly 4.3.1.2. Navíc může vnitřní předpis zahrnovat technickou dokumentaci kamerového systému, která však zpravidla nebývá přístupná všem zaměstnancům, nýbrž pouze pověřenému úzkému okruhu zaměstnanců, kteří zajišťují zpracování osobních údajů a starají se o jejich zabezpečení.[152]

4.4.3 Zpracovatelská smlouva

Povinnost uzavření specifické smlouvy o zpracování dopadá na toho zaměstnavatele, který správou kamerového systému pověří namísto svého

[151] Tamtéž.
[152] HAVEL A PARTNEŘI. Instalace a provoz kamerového systému z pohledu GDPR a zákoníku práce – část I. [online]. ŠUCHMAN, Jaroslav a Ján JAROŠ. 2022 [cit. 2024-03-21]. Dostupné z: https://www.havelpartners.blog/instalace-a-provoz-kameroveho-systemu-z-pohledu-gdpr-a-zakoniku-prace-cast-i.

zaměstnance externí osobu či společnost. GDPR připouští vedle zpracovatelské smlouvy též jiný právní akt, nicméně v kontextu kamerových systémů je velmi nepravděpodobné, že byl využit jiný právní akt, než jakým je zpracovatelská smlouva. Je nutné podotknout, že se musí jednat o správu zahrnující přístup ke kamerovým záznamům či online monitoringu nebo takto pověřená externí osoba musí mít možnost provádění operací s kamerovým systémem souvisejících. V případě, že zaměstnavatel pověří externí firmu pouze k zajištění technické stránky provozu kamerového systému, není uzavření zpracovatelské smlouvy nutné.[153]

Smlouva nemusí být uzavřena jako samostatný dokument, ale pouhé stanovení povinnosti řídit se interním předpisem by mohlo být dle GDPR považováno za nedostatečné. Tato konkrétní smlouva by tedy dle GDPR měla jasně určovat, jaký typ a kategorie osobních údajů mohou být zpracovány, předmět zpracovávání osobních údajů – tedy kamerový systém (počet, umístění, druh objektu), jak dlouho mohou být uchovávány, jak mají být chráněny, jaký je účel a povaha zpracování a též výčet operací prováděných zpracovatelem, včetně časového plánu. Rovněž by měla definovat práva a povinnosti správce i zpracovatele a neměla by chybět ani doba na kterou je zpracovatelská smlouva mezi externí firmou a zaměstnavatelem uzavřena.[154]

Na závěr je třeba uvést, že smlouva by měla mít písemnou podobu. Avšak na rozdíl od interního předpisu nemusí zaměstnavatel disponovat jejím fyzickým vyhotovením a postačí pouze elektronická verze. Na druhou stranu, pokud by měl zpracovatel sídlo v třetí zemi, měla by být smlouva ve fyzické podobě vyhotovena. To především z důvodu opatrnosti správce, protože daný stát může mít odlišnou úpravu od té evropské, a tudíž by elektronická podoba zde nemusela být postavena na roveň té elektronické.[155]

[153] Tamtéž.
[154] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024. S. 24-25. [cit. 2024-03-21]. Dostupné z: https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf.
[155] NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7. s. 100.

5 ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

ÚOOÚ je součástí evropské sítě nezávislých orgánů veřejné správy, které jsou nadány dozorujícími a vyšetřujícími pravomocemi směřujícími k zajištění dodržování právních předpisů v oblasti ochrany osobních údajů a souvisejících práv jednotlivců.[156]

V České republice byl ÚOOÚ zřízen zákonem o ochraně osobních údajů dne 1. června 2000 a prvním předsedou se stal na návrh Senátu v září téhož roku RNDr. Karel Neuwirt.[157]

Jako dozorčí orgán s kompetencemi ústředního správního úřadu s obecnou působností v oblasti ochrany osobních údajů je jediným dozorovým orgánem v České republice. Mezi jeho stěžejní pravomoc patří monitorování a dohled nad dodržováním normativních právních v předpisů v oblasti ochrany osobních údajů. V tomto kontextu disponuje kompetencí vydávat autoritativní správní rozhodnutí, které je povětšinou výsledkem výkonu kontroly, která je primárním nástrojem pro výkon monitorování a dohledu ÚOOÚ. Kontrola je vykonávána buďto na základě kontrolního plánu nebo na základě stížnosti subjektu údajů či jiných kvalifikovaných podnětů. Zaměstnanec ÚOOÚ je tuto kontrolu oprávněn provést na základě písemného pověření a má povinnost se při její realizaci držet norem stanovených kontrolním řádem, zákonem a odpovědnosti za přestupky a subsidiárně též správním řádem. V případě zjištění rozporu mezi skutečností a stavem presumovaným právní úpravou přechází výkon správního dozoru do fakultativní fáze nápravné či sankční.[158] V této fázi je ÚOOÚ oprávněn udělit pokutu či jinou sankci, které mají za cíl potrestat subjekt, který se porušení předpisů dopustil, ale neopominutelná je také funkce preventivní, jež má působit také obecně na další subjekty.

Další činnost, kterou se ÚOOÚ zabývá, je činnost konzultační poradenská a činnost osvětová. Konzultační role ÚOOÚ má vést k přiblížení problematiky

[156] EVROPSKÁ KOMISE. Co jsou to úřady pro ochranu osobních údajů? [online]. [cit. 2024-03-17]. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_cs.
[157] ÚOOÚ. Historie úřadu [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/urad/historie-uradu.
[158] ÚOOÚ. Ochrana osobních údajů [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/cinnost/ochrana-osobnich-udaju

ochrany osobních údajů široké veřejnosti. Za tímto účelem je v rámci organizační struktury ÚOOÚ zřízen odbor předávání, akreditací a konzultací se speciálním oddělením věnujícím se konzultační činnosti[159], které také provozuje dva dny v týdny informační telefonní linku, která slouží k rychlým dotazům ohledně problematiky GDPR.[160] ÚOOÚ nabízí také možnost osobních konzultací, která je zřejmě nejúčinnější a nejrychlejší variantou při řešení složitějších otázek. Výstupy z konzultací, které by mohly být obecně přínosné i pro další správce poté zveřejňuje ÚOOÚ na svých webových stránkách, případně ve výjimečných případech ÚOOÚ organizuje veřejnou diskuzi k danému tématu.[161] V neposlední řadě ÚOOÚ koná v rámci osvětové činnosti též odborné semináře. Posledním takto organizovaným seminářem byl seminář konaný dne 6. března 2024 k nové Metodice týkající se kamerových systémů, přičemž tohoto se semináře se zúčastnilo téměř 600 odborníků věnující se problematice provozování kamerových systémů s ohledem na ochranu osobních údajů.[162]

V současné době stojí ve vedení úřadu od září roku 2020 Mgr. Jiří Kaucký, kterého do funkce předsedy ÚOOÚ jmenoval dnes již bývalý prezident Miloš Zeman.[163]

[159] ÚOOÚ. Organizační struktura Úřadu, platná k 1.3.2024 [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/urad/organizacni-struktura
[160] ÚOOÚ. Kontakt [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/kontakt
[161] VIDRNA, Jan a Zdeněk KOUDELKA. Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců. V Praze: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7.S.153.
[162] ÚOOÚ. Semináře ÚOOÚ ke kamerovým systémům se zúčastnilo na 600 expertů [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/novinky/vse/seminare-uoou-ke-kamerovym-systemum-se-zucastnilo-600-expertu
[163] ÚOOÚ. Životopis předsedy Jiřího Kauckého [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/urad/organizacni-struktura/zivotopis-predsedy-jiriho-kauckeho

6 JUDIKATURA A DOSAVADNÍ PRAXE

Tato kapitola má za cíl zaměřit se na klíčové případy, které formulovaly právní rámec a ovlivňují dosavadní praxi v oblasti ochrany soukromí na pracovišti.

Judikatura jako taková poskytuje cenný vhled do toho, jak soudy vykládají a aplikují zákony na konkrétní situace vytvořené pracovním prostředím. Představím zde nejdůležitější rozhodnutí ESLP[164] zabývající se kamerovými systémy na pracovišti. Pro komplexní přehled budou rovněž uvedeny zásadní případy, které byly řešeny na úrovni vnitrostátních soudů. Na závěr budou zhodnoceny důsledky těchto rozhodnutí a jejich vliv na práva a povinnosti jak zaměstnanců, tak zaměstnavatelů.

6.1 Lopéz Ribalda proti Španělsku

Mezi relativně nové rozsudky s velkým významem v této oblasti patří rozsudek ESLP č. 1874/13 ze dne 17. října 2019 ve věci Lopéz Ribalda a ostatní proti Španělsku.

V tomto případě se ESLP zabýval případem pěti zaměstnanců španělského maloobchodního řetězce, kteří byli vystaveni dohledu prostřednictvím kamerového systému s cílem detekovat potenciální krádeže. Avšak, zaměstnavatel neuposlechl povinnost informovat zaměstnance o tomto sledování, konkrétně o existenci skrytých kamer, ačkoliv taková povinnost je stanovena španělským vnitrostátním právem. Zaměstnanci byli informováni pouze o viditelných kamerách, nikoliv o těch skrytých.

Po desetidenním monitoringu prostoru pokladen pomocí skrytých kamer bylo zjištěno, že několik zaměstnanců se aktivně podílelo na krádeži zboží. Dále bylo odhaleno, že tito zaměstnanci nejenže spolupracovali při páchání těchto krádeží, ale také asistovali dalším osobám při jejich uskutečňování. V důsledku toho, bylo propuštěno čtrnáct zaměstnanců včetně stěžovatelek. Španělské soudy shledaly žaloby stěžovatelek proti propuštění jako nedůvodné a potvrdily oprávněný zájem zaměstnavatele na kamerovém sledování.

[164] Mezi další klíčové rozsudky ESLP v oblasti ochrany soukromí zaměstnance na pracovišti řadíme například rozsudek ve věci Akhlyustin proti Rusku a Barbulescu proti Rumunsku.

Senát třetí sekce ESLP však v první fázi svého rozhodování dospěl k odlišnému závěru. Ve svém rozsudku ze dne 9. ledna 2018 potvrdil, že došlo k porušení článku 8 Evropské úmluvy o lidských právech a svobodách, čímž vyhověl stěžovatelkám. Senát dospěl k tomuto závěru na základě porušení informační povinnosti zaměstnavatele, kterou stanovuje španělské právo, a také kvůli nepřiměřeně širokému rozsahu skrytého sledování. Dále senát kritizoval absenci jasného vymezení časového rozsahu skrytého monitoringu a konkrétního počtu zaměstnanců, kteří měli být sledování podrobeni.[165]

Nicméně, po dalším posouzení případu velkým senátem ESLP došlo k přehodnocení původního stanoviska senátu třetí sekce ESLP. Ve druhé fázi rozhodovacího procesu velký senát v rozsudku ze dne 17. října 2019 určil, že v daném případě nedošlo k porušení příslušného článku zaručujícího ochranu soukromí.

Podle velkého senátu ESLP bylo jednání zaměstnavatele, který nařídil skryté sledování pokladen na základě důvodného podezření z krádeží zaměstnanci, legitimní. Toto podezření vyplynulo ze zjištěného poklesu tržeb. Senát považoval rozsah sledování konkrétních oblastí a osob za přiměřený vzhledem k velikosti zjištěné ztráty a také vzhledem k použitému prostředku – kamerovým systémům. Senát dále konstatoval, že záznamy byly pořizovány pouze po nezbytně nutnou dobu k identifikaci pachatelů a byly využity výhradně pro účely odhalení tohoto protiprávního jednání. Na základě těchto důvodů velký senát ESLP rozhodl poměrem hlasů 14:3, že nedošlo k porušení článku 8 Evropské úmluvy o lidských právech a svobodách.[166]

6.2 Antonović a Mirković proti Černé Hoře

Stěžovateli v této věci byli vyučujícími na fakultě matematiky na Černohorské univerzitě v Podgorici. Podnětem k podání stížnosti k ESLP bylo oznámení podané začátkem roku 2011 děkanem fakult, o zavedení kamerového systému se záznamem do poslucháren na fakultě. Cílem monitoringu

[165] Rozsudek Třetí sekce ESLP ve věci Lopéz Ribalda a ostatní v. Španělsko, ze dne 9. ledna 2018, stížnost č. 1874/13.
[166] Rozsudek Velkého senátu ESLP ve věci Lopéz Ribalda a ostatní v. Španělsko, ze dne 19. 10. 2019, stížnost č. 1874/13.
Kamerové systémy na pracovišti [online]. LOBOTKA, Andrej. 2024 [cit. 2024-03-28]. Dostupné z: https://www.gdpr.cz/kamerove-systemy-na-pracovisti.

přednáškových místností bylo zajištění majetku univerzity, ochrana osob a sledování výuky. Přičemž k získaným záznamům měl přístup výhradně děkan fakulty a tyto záznamy měly být archivovány po dobu jednoho roku. Stěžovatelé u vnitrostátních soudů se svou argumentací neuspěli, a tak následně v říjnu roku 2013 proti monitoringu v posluchárnách podali stížnost k ESLP.

ESLP v předchozím rozhodnutí Köpke proti Německu konstatoval, že skryté sledování na pracovišti představuje značný zásah do soukromí. Tento postoj si ESLP udržel i v případě Antović a Mirković proti Černé Hoře, a to i přes to, že v tomto případě byli vyučující o sledování informováni. ESLP dále konstatoval, že soudy v Černé Hoře svým rozhodováním porušily vnitrostátní předpisy, upravující ochranu osobních údajů. Nezákonnost těchto rozhodnutí spatřil ESLP především v tom, že soudy nepovažovaly sledování na pracovišti za zásah do soukromí stěžovatelů.

Na závěr ESLP upozornil na to, že sledování nesplnilo účel, který byl předpokládán vnitrostátním předpisem. Dále sice vnitrostátní úprava povolovala monitorování veřejných institucí, jakou je i univerzita, avšak zákon se omezoval pouze na vstupy do předmětných budov, nikoliv posluchárny jako tomu bylo v této věci. Rovněž ještě ESLP zmiňuje nenaplnění legitimního cíle monitoringu předpokládané vnitrostátním předpisem.

Rozsudkem ze dne 28. listopadu 2017 dal senát druhé sekce ESLP dotčeným akademickým pracovníkům za pravdu, přiznal jim náhradu škody a konstatoval v poměru hlasů 4:3 porušení článku 8 Evropské úmluvy o lidských právech a svobodách.[167]

6.3 Judikatura vnitrostátních soudů

V oblasti ochrany soukromí zaměstnanců, zejména s ohledem na použití kamerových systémů, není domácí judikatura příliš rozsáhlá. Nicméně, tato judikatura poskytuje nezbytný kontext a doplňuje evropské právní předpisy a rozhodnutí v této oblasti.

[167] Rozsudek Druhé sekce ESLP ve věci Antović a Mirković proti Černé Hoře, ze dne 28. listopadu, stížnost č. 70838/13.
MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3. s. 381.

Nejčastěji se v této oblasti objevují rozsudky v rámci správního soudnictví. To je logické, protože do působnosti správního soudnictví spadají žaloby dožadující se přezkoumání rozhodnutí ÚOOÚ.

Jedním z významných rozhodnutí, které se týká problematiky monitorování pracovišť pomocí kamerových systémů, je rozhodnutí NSS ze dne 23. srpna 2013, sp. zn. 5 As 158/2012. Toto rozhodnutí se zaměřilo na otázku zákonnosti instalace kamerového systému s funkcí záznamu v hotelu vyšší kategorie.[168]

V daném hotelu bylo nainstalováno celkem 16 kamer se záznamem, které monitorovaly nejen veřejné prostory jako lobby nebo vstup do hotelu, ale také provozní části hotelu, kam měli přístup pouze zaměstnanci hotelu. Soud konstatoval, že tímto zaměstnavatel podrobil zaměstnance otevřenému sledování bez naplnění zákonné podmínky vyplývající z § 316, odst. 2, 3 zákoníku práce. Soud dále uvedl, že činnost spočívající v provozu hotelu není činností povahou nijak zvláštní, a proto není zapotřebí kontrolu nad zaměstnanci vykonávat prostřednictvím kamerového systému, který významně zasahuje do osobnostní sféry člověka.

Soud dále konstatoval, že k zavedení kamerových systémů je možné přistoupit pouze v případě, pokud alternativní prostředky, které jsou svou povahou schopny menšího zásahu do soukromí než kamerové systémy, selhaly a nebyly schopny naplnit stanovený účel.

NSS v tomto rozsudku také stanovil podmínky monitoringu zaměstnance na pracovišti. Sledování zaměstnance na pracovišti je možné jen v nezbytně nutném případě spočívajícím v ochraně zdraví osob nebo majetku zaměstnavatele, přičemž zaměstnanci musí být s touto kontrolou předem seznámeni. Tato informace zahrnuje rozsah a způsob provádění kontroly, tedy prostředky, jakými je kontrola prováděna. Monitoring by se měl zaměřit především na majetek zaměstnavatele, tedy pokud je to možné, kamera by neměla ve svém záběru zaznamenávat zaměstnance. A v neposlední řadě, i přes splnění těchto podmínek,

[168] PRÁVNICKÁ FAKULTA, MASARYKOVA UNIVERZITA. Ochrana osobnosti zaměstnanců v soudní praxi [online]. HROMADA, Miroslav. 2018 [cit. 2024-03-29]. Dostupné z: https://www.law.muni.cz/sborniky/pracpravo2017/files/008.html.

zaměstnavatel nesmí kamerový systém instalovat na místech sloužících k hygieně a odpočinku zaměstnanců.[169]

Obdobně NSS ve svém rozhodnutí ze dne 20. prosince 2017, sp. zn. 10 As 245/2016, bylo konstatoval, že povaha práce řidiče autobusu nepředstavuje závažný důvod, který by opravňoval zaměstnavatele k monitorování kabiny autobusu pomocí kamerových systémů podle § 316, odst. 2, 3 zákoníku práce.

Toto rozhodnutí bylo učiněno navzdory argumentům dopravní společnosti, která tvrdila, že činnost řidiče autobusu lze zařadit pod tento paragraf vzhledem k vysoké odpovědnosti řidiče za množství přepravovaných životů.

Soud v tomto kontextu uvedl, že pokud by přijal tento argument, musel by tuto charakteristiku přiznat všem formám automobilové dopravy, protože jakýkoliv řidič může způsobit škodu na zdraví nebo majetku jakékoliv třetí osoby, a to i v značném rozsahu.[170]

6.4 Východiska předmětných rozhodnutí

Z analýzy uvedených judikátů lze dle mého názoru vyvodit, že soudy všech instancí jednoznačně podporují práva slabší strany, tj. zaměstnance, a přenášejí právo na ochranu soukromí i do pracovního prostředí.

Nicméně existuje určitý limit ochrany soukromí zaměstnance, který je relevantní v případě, kdy zaměstnavatel má důvodné podezření, že se zaměstnanec dopouští protiprávního jednání. Domnívám se však, i s ohledem na výše rozebrané rozsudky, že toto podezření by mělo být opřeno o konkrétní doložitelné skutečnosti jako jsou například výsledky účetní závěrky nebo inventury zboží. Nelze připustit, aby zaměstnavatel monitoroval pracoviště skrytě bez předchozího oznámení, pokud by informace o protiprávním jednání získal například pouze od jednoho ze zaměstnanců.

V případě, že zaměstnavatelovo podezření bude opřeno o doložitelné skutečnosti, může zavést skrytý monitoring pouze po nezbytně nutnou dobu k odhalení nepoctivého zaměstnance. Získané záznamy by pak pro dodržení zákonnosti jejich pořizování měly být použity pouze k deklarovanému účelu, tedy k usvědčení zaměstnance.

[169] Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012.
[170] Rozsudek Nejvyššího správního soudu ze dne 20. 12. 2017, sp. zn.10 As 245/2016.

Tato praxe je v souladu s rozhodnutím soudů a je považována za respektující k právům zaměstnanců na ochranu soukromí i přes absenci předchozího splnění oznamovací povinnosti stanovené jak v GDPR, tak v zákoníku práce.

7 PRÁVNÍ ÚPRAVA DE LEGE FERENDA

S ohledem na provedený rozbor kamerových systémů na pracovišti v rámci této práce se mi jako klíčový problém jeví nedostatečná konkrétnost, která ovlivňuje právní úpravu těchto systémů.

Metodika ÚOOÚ konečně stanovila, že i kamerové systémy bez záznamu zpracovávají osobní údaje v režimu GDPR, tedy za předpokladu, že kamera umožňuje zaměstnance identifikovat. Tento postoj ÚOOÚ byl potvrzen ve výroční zprávě pro rok 2023.[171] Je však důležité zdůraznit, že tato interpretace přišla až po téměř šesti letech od účinnosti GDPR.

Velkou neznámou, která by se dle mého názoru zasloužila konkrétnější úpravu je celková kontrola a monitoring nad zaměstnancem. V současném zákoníku práce existuje totiž pouze jediný paragraf, který se touto problematikou zabývá. Tato strohost ve spojení se značně výkladově širokými a nejasnými pojmy jako je již řešený „*závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele*“ vytváří v zaměstnavateli značnou právní nejistotu. Domnívám se, že by tento pojem měl být jasně definován zákonodárcem. Z dosavadní judikatury soudů vyplývá pouze to, že tímto závažným důvodem není činnost řidiče autobusu ani provoz hotelového zařízení, což mi připadá více než nedostatečné. Shoda ve vymezení této podmínky, jak již bylo popsáno, v odborné veřejnosti také nepanuje.

Metodika vydaná v letošním roce ÚOOÚ je zajisté velkým počinem, který přinese více jasnosti do oblasti kamerových systémů. Nicméně je důležité si uvědomit, že se jedná pouze o právně nezávazný dokument vydaný dozorovým orgánem, který se zaměřuje obecně na kamerové systémy. Zaměstnavatelům tak neposkytuje plnou právní jistotu ohledně zákonnosti instalovaného kamerového systému na pracovišti.

[171] ÚOOÚ. Výroční zpráva 2023 [online]. s. 36. [cit. 2024-03-29]. Dostupné z: https://uoou.gov.cz/media/vyrocni-zpravy/vz2023-elektronicka-verze.pdf.

Z hlediska dodržování právních předpisů týkajících se kamerových systémů na pracovišti by bylo vhodné, kdyby zákonodárce reagoval na výzvu obsaženou v článku 88 nařízení GDPR. Tento článek přímo vyzývá členské státy, aby buďto prostřednictvím kolektivních smluv nebo právních předpisů upravily zpracování osobních údajů v souvislosti se zaměstnáním, zejména co se týče systémů monitoringu na pracovišti.[172]

Domnívám se, že vytvoření právně závazného dokumentu, který by se obecně věnoval možnostem monitoringu na pracovišti a detailněji rozebíral postupy v závislosti na zvoleném prostředku kontroly, by představovalo významný legislativní krok. Tuto iniciativu by ocenili nejen zaměstnavatelé, ale také dozorový orgán ÚOOÚ. Konkrétnější postupy na zákonné úrovni by mohly vést k úbytku kamerových systémů a dalších monitorovacích nástrojů nejen na pracovišti, ale i na dalších specifických místech, což by přispělo k odlehčení zátěže pro ÚOOÚ. Je tedy dle mého názoru žádoucí, aby byli tyto postupy jasněji definovány a upraveny v legislativě.

Dalším možným opatřením, které by pomohlo snížit neoprávněné zásahy do soukromé sféry zaměstnanců v souvislosti s instalací kamerových systémů na pracovišti, je zavedení zákonné povinnosti zřízení pověřence pro ochranu osobních údajů. Tento krok by byl v souladu s článkem 37 nařízení GDPR.[173]

Každý zaměstnavatel, který chce provádět kontrolu svých zaměstnanců, ať už prostřednictvím kamerového systému nebo jiného nástroje zpracovávajícího osobní údaje, by měl mít pověřence, jehož úkolem by bylo minimalizovat nelegální zásahy do soukromí zaměstnanců. Pro menší zaměstnavatele by bylo samozřejmě možné namísto interního pověřence tuto funkci externalizovat na specializované jednotlivce nebo zpracovatelské firmy.

[172] Článek 88, odst. 1, 2 GDPR.
[173] Článek 37 GDPR.

ZÁVĚR

Tato diplomová práce se zaměřila na komplexní analýzu problematiky kamerových systémů na pracovišti. Byl proveden detailní rozbor právní úpravy této oblasti s cílem poskytnout čtenáři autentický obraz o implementaci principů ochrany osobních údajů do pracovněprávních vztahů.

V první kapitole této diplomové práce byly vymezeny nejdůležitější základní pojmy spojené s právem na ochranu soukromí v kontextu této práce, včetně přiblížení pojmu kamerového systému a kamerového sledování bez zpracování osobních údajů, které neoddělitelně souvisí se stupněm identifikace osoby zaměstnance.

Druhá část společně s částí třetí byly zaměřeny na rozlišení kamerových systémů s funkcí záznamu a bez něj. Ve čtvrté části byl detailně popsán vývoj názoru ÚOOÚ na problematiku zpracování osobních údajů právě pomocí kamerových systémů bez záznamu.

Čtvrtá část byla věnována konkrétním podmínkám, které je zaměstnavatel nucen dodržet, aby instalace kamerového systému byla v souladu se zákonem, přičemž při vymezení těchto podmínek byl brán v potaz jak současný zákoník práce, tak nařízení GDPR. Konkrétně byly rozebrány základní zásady pro zpracování osobních údajů, které, jak již bylo zmíněno v předchozích kapitolách, je nedílnou součástí každého kamerového systému. Dále také jednotlivé právní tituly opravňující zaměstnavatele k instalaci kamer, jakožto i detailní seznámení s právy zaměstnanců, které jim v souvislosti se zpracováním osobních údajů vznikají. A na závěr této kapitoly byl čtenář seznámen s několika potřebnými dokumenty pro zavedení kamerového systému na pracovišti.

Pátá kapitola věnovala pozornost Úřadu pro ochranu osobních údajů, vymezila jeho hlavní činnosti, jakožto i působnost v kontextu kamerových systémů.

Šestá kapitola čtenáři přiblížila dosavadní praxi soudů na vnitrostátní i evropské úrovni, přičemž na závěr bylo zaujmuto východisko jednoznačné podpory práv na soukromí zaměstnance ze strany soudů všech instancí.

V závěrečné sedmé kapitole, po důkladné analýze provedené touto diplomovou prací, bylo autorem doporučeno několik návrhů na legislativní posun

v této oblasti. Zejména pak se zaměřením na definování „*závažného důvodu spočívajícího ve zvláštní povaze zaměstnavatele*“, využití článku 88 GDPR pro vytvoření speciálního zákonného předpisu věnují se zavedením konkrétních postupů pro zavedení kamerových systémů nejen na pracovišti. Rovněž jako stanovení zákonné povinnosti zřízení funkce pověřence pro ochranu osobních údajů na pracovištích, jež kamerových systémů ke kontrole svých zaměstnanců využívají.

RESUMÉ

This thesis provided a comprehensive overview of the issue of camera systems in the workplace. It conducted a detailed analysis of the legal adjustment of this issue to provide an authentic picture of the implementation of personal data protection principles into labor law relationships.

The first chapter defined key terms associated with the right to privacy in the context of this work, including the concept of a camera system and camera surveillance without personal data processing, which is related to the degree of employee identification.

The second and third parts focused on distinguishing camera systems with and without a recording function. The fourth part described the development of the Office for Personal Data Protection's opinion on the issue of personal data processing using camera systems without recording.

The fourth part was dedicated to specific conditions that the employer must comply with for the installation of a camera system to be legal. The fifth chapter focused on the Office for Personal Data Protection, its main activities, and jurisdiction in the context of camera systems.

The sixth chapter introduced the current practice of courts at the national and European level, emphasizing the unequivocal support of employee privacy rights by courts of all instances.

In the final seventh chapter, after a thorough analysis, several proposals for legislative shift in this area were recommended. Specifically, focusing on defining the "serious reason consisting of the special nature of the employer", using Article 88 of the GDPR to create a special legal regulation dealing with the introduction of specific procedures for the introduction of camera systems not only in the workplace. Also, it was recommended to establish a legal obligation to establish the function of a data protection officer in workplaces that use camera systems to control their employees.

This work thus presents a comprehensive overview of the issue of camera systems in the workplace and presents proposals for further legislative development in this area.

SEZNAM PRAMENŮ A ODBORNÉ LITERATURY

Česká odborná literatura

1. BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů v aplikační praxi: vybrané otázky. 3. vyd. Praha: Linde Praha, 2013. Praktická právnická příručka. ISBN 978-80-86131-96-2.
2. BĚLINA, Miroslav. Zákoník práce: komentář. 4. vydání. V Praze: C.H. Beck, 2023. Velké komentáře. ISBN 978-80-7400-951-8.
3. FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. GDPR: hmotné a procesní aspekty prakticky. V Praze: C.H. Beck, 2019. Právní praxe. ISBN 978-80-7400-762-0.
4. HŮRKA, Petr. Pracovní právo. 5. vyd. Plzeň: Aleš Čeněk, 2023. ISBN 978-80-7380-33-1.
5. JANEČKOVÁ, Eva a Václav BARTÍK. Kamerové systémy v praxi. Linde Praha, 2011. ISBN 978-80-7201-850-5.
6. MORÁVEK, Jakub. Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy. Wolters Kluwer, 2019. ISBN 978-80-7598-587-3.
7. NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.
8. NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.
9. PICHRT, Jan. Zákoník práce: Zákon o kolektivním vyjednávání. 2. vydání. Praha: Wolters Kluwer, 2022. Praktický komentář. ISBN 978-80-7676-388-3.
10. ŠIMEČKOVÁ, Eva. Nežádoucí chování na pracovišti. Leges, 2023. ISBN 978-80-7502-698-9.
11. 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.
12. VIDRNA, Jan a Zdeněk KOUDELKA. Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců. V Praze: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7.
13. WAGNEROVÁ, Eliška. Listina základních práv a svobod: komentář. 2., doplněné a aktualizované vydání. Praha: Wolters Kluwer, 2023. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7676-747-8.
14. ZAHRADNÍČEK, Jaroslav. Ochrana osobnosti v pracovněprávních vztazích. Praha: Leges, 2019. Teoretik. ISBN 978-80-7502-373-5.
15. ŽŮREK, Jiří. GDPR v personalistice. Olomouc: ANAG, [2019]. Práce, mzdy, pojištění. ISBN 978-80-7554-210-6.

Odborné články

1. PAVLÍK, Pavel. Biometrie jako základ současné i budoucí identifikace a autentizace. Kontakt. 2007, (2), 427-430. ISSN 1212–4117.
2. WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. HARVARD LAW REVIEW. 15. 12.1890n. l., 1890(5), 193-220.
3. NONNEMANN, František: Soukromí na pracovišti, Právní rozhledy. Č. 7/2015, s. 229

Právní předpisy

1. Listina základních práv Evropské unie
2. Nařízení Evropského parlamentu a Rady (EU) 2016/676 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
3. Sdělení č. 209/1992 Sb., o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto úmluvu navazujících
4. Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 14. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
5. Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních údajů
6. Usnesení č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, Předsednictva České národní rady
7. Ústavní zákon č. 1/1993 Sb., Ústava České republiky, České národní rady
8. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
9. Zákon č. 110/2019 Sb., o zpracování osobních údajů
10. Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich
11. Zákon č. 251/2005 Sb., o inspekci práce
12. Zákon č. 255/2012 Sb., o kontrole (kontrolní řád)
13. Zákon č. 262/2006 Sb., zákoník práce
14. Zákon č. 40/2009 Sb., trestní zákoník
15. Zákon č. 500/2004 Sb., správní řád
16. Zákon č. 89/2012 Sb., občanský zákoník

Judikatura

1. Rozsudek Druhé sekce ESLP ve věci Antović a Mirković proti Černé Hoře, ze dne 28. listopadu, stížnost č. 70838/13
2. Rozsudek Nejvyššího soudu ze dne 26. 11. 2015 sp. zn. 21 Cdo 4596/2014
3. Rozsudek Nejvyššího správního soudu ze dne 20. 12. 2017, sp. zn.10 As 245/2016.
4. Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012
5. Rozsudek Nejvyššího správního soudu ze dne 25. 02. 2015, č.j. 1 As 113/2012-133

6. Rozsudek německého Spolkového ústavního soudu ze dne 15.12.1983, sp. zn. BVerfGE 65,1. Odkazovaný v nálezu Ústavního soudu ze dne 22.3.2011, sp. zn. Pl. ÚS 24/10
7. Rozsudek Třetí sekce ESLP ve věci Lopéz Ribalda a ostatní v. Španělsko, ze dne 9. ledna 2018, stížnost č. 1874/13
8. Rozsudek Velkého senátu ESLP ve věci Lopéz Ribalda a ostatní v. Španělsko, ze dne 19. 10. 2019, stížnost č. 1874/13

Internetové zdroje

1. BURIAN, David. ÚOOÚ. Seminář k metodice návrhu a provozování kamerových systémů [online]. 2024. [cit. 2024-03-11]. Dostupné z: https://uoou.gov.cz/media/seminareuoou/prezentace/2024-03-06-seminar-uoou-metodika-ke-kameram.pdf.
2. EVROPSKÁ KOMISE. Co jsou to úřady pro ochranu osobních údajů? [online]. [cit. 2024-03- 17]. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/reform/what-aredata-protection-authorities-dpas_cs.
3. HAVEL A PARTNEŘI. Instalace a provoz kamerového systému z pohledu GDPR a zákoníku práce – část I. [online]. ŠUCHMAN, Jaroslav a Ján JAROŠ. 2022 [cit. 2024-03-21]. Dostupné z: https://www.havelpartners.blog/instalace-a-provoz-kameroveho-systemu-z-pohledu-gdpr-azakoniku-prace-cast-i.
4. HOSPODÁŘSKÉ NOVINY. Soukromí v práci ve světle evropské judikatury [online]. ZAHRADNÍČEK, Jaroslav. 2019 [cit. 2024-03-01]. Dostupné z: https://hn.cz/c1-66611530- soukromi-v-praci-ve-svetle-evropske-judikatury#viz8.
5. HUBACZKOVÁ, Gabriela. Pojem pracoviště z pohledu bezpečnosti práce [online]. [cit. 2024- 02-23]. Dostupné z: https://www.bozpinfo.cz/pojem-pracoviste-z-pohledu-bezpecnosti-prace.
6. Instalace bezpečnostních kamer musí být v souladu s ochranou osobních údajů. MIKUŠOVÁ, Hana. Právo 21 [online]. 2021 [cit. 2024-02-29]. Dostupné z: https://pravo21.cz/pravo/instalacebezpecnostnich-kamer-musi-byt-v-souladu-s-ochranou-osobnich-udaju.
7. Jak používat kamery na pracovišti. GEMBALOVÁ, Kristýna. Právní prostor [online]. 2024 [cit. 2024-03-19]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/jak-pouzivatkamery-na-pracovisti.

8. Kamerové systémy na pracovišti [online]. LOBOTKA, Andrej. 2024 [cit. 2024-03-28]. Dostupné z: https://www.gdpr.cz/kamerove-systemy-na-pracovisti.
9. KAMEROVÉ SYSTÉMY, NOVINKY, TECHNOLOGIE [online]. [cit. 2024-02-25]. Dostupné z: https://www.securityblog.cz/2023/12/29/axis-predstavuje-inovativni-multisenzorove-kamery-sumelou-inteligenci-pro-komplexni-pokryti-sirokych-ploch-v-rozliseni-az-4x4k/.
10. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Kamerové systémy [online]. [cit. 2024-02- 24]. Dostupné z: https://www.mvcr.cz/clanek/kamerove-systemy.aspx.
11. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Ministerstvo vnitra rozšíří zabezpečení Letiště Václava Havla o 145 kamer s automatickým rozpoznáváním obličejů [online]. 2019 [cit. 2024-02-25]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-rozsiri-zabezpeceniletiste-vaclava-havla-o-145-kamer-s-automatickym-rozpoznavanim-obliceju.aspx.
12. MORÁVEK, Jakub. KONTROLA A SLEDOVÁNÍ ZAMĚSTNANCŮ – VÝKLAD § 316 ZPR. Právní rozhledy [online]. Praha, 2017(17), 573 [cit. 2024-03-05]. Dostupné z: https://app.beckonline.cz/bo/chapterview-document.
13. NATIONAL INSTITUTE OF JUSTICE. Research on Body-Worn Cameras and Law Enforcement [online]. 2022 [cit. 2024-02-25]. Dostupné z: https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement.
14. NONNEMANN, František. Nová metodika ÚOOÚ ke kamerám: Jste v souladu? GDPR.cz [online]. 2014 [cit. 2024-03-05]. Dostupné z: https://www.gdpr.cz/nova-metodika-uoou-kekameram-jste-v-souladu.
15. PRÁVNICKÁ FAKULTA, MASARYKOVA UNIVERZITA. Ochrana osobnosti zaměstnanců v soudní praxi [online]. HROMADA, Miroslav. 2018 [cit. 2024-03-29]. Dostupné z: https://www.law.muni.cz/sborniky/pracpravo2017/files/008.html.
16. RÖSLEROVÁ, Karolína. *Sledování zaměstnanců v kontextu Obecného nařízení o ochraně osobních údajů* [online]. Praha, 2020 [cit. 2024-03-31]. Dostupné z: https://dspace.cuni.cz/bitstream/handle/20.500.11956/118768/120362835.pdf?sequence=1&isAllowed=y. Diplomová práce. Univerzita Karlova, Právnická fakulta, Katedra pracovního práva a práva sociálního zabezpečení.

17. ŠRAJ, Jan. Zásady činnosti veřejné správy [online]. Olomouc, 2013 [cit. 2024-03-31]. Dostupné z: https://theses.cz/id/m5e3e1/. Diplomová práce. UNIVERZITA PALACKÉHO V OLOMOUCI, právnická fakulta. Vedoucí práce JUDr. Ing. Filip Dienstbier, Ph.D
18. ÚOOÚ. Historie úřadu [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/urad/historie-uradu
19. ÚOOÚ. Kontakt [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/kontakt
20. ÚOOÚ. Ochrana osobních údajů [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/cinnost/ochrana-osobnich-udaju
21. ÚOOÚ. Organizační struktura Úřadu, platná k 1.3.2024 [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/urad/organizacni-struktura
22. ÚOOÚ. Semináře ÚOOÚ ke kamerovým systémům se zúčastnilo na 600 expertů [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/novinky/vse/seminare-uoou-ke-kamerovymsystemum-se-zucastnilo-600-expertu
23. ÚOOÚ. Úřad pro ochranu osobních údajů zveřejnil novou Metodiku k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů. [online]. [cit. 2024-03-01]. Dostupné z: https://uoou.gov.cz/novinky/vse/nova-metodika-uradu-ke-kamerovym-systemum
24. ÚOOÚ. Životopis předsedy Jiřího Kauckého [online]. [cit. 2024-03-17]. Dostupné z: https://uoou.gov.cz/urad/organizacni-struktura/zivotopis-predsedy-jiriho-kauckeho
25. Vysvětlení označení a zkratek při bezpečnostních kamerách [online]. [cit. 2024-02-24]. Dostupné z: https://www.efeel.cz/vysvetleni-oznaceni-a-zkratek-pri-bezpecnostnich-kamerach.
26. Vztahuje se GDPR i na online kamery? NONNEMANN, František. Epravo.cz [online]. 2020 [cit. 2024-02-29]. Dostupné z: https://www.epravo.cz/top/clanky/vztahuje-se-gdpr-i-na-onlinekamery.
27. ZEPCAM. Výhody osobních kamer pro policii a orgány činné v trestním řízení [online]. [cit. 2024-02-25]. Dostupné z: https://zepcam.com/cs/vyhody-telesnych-kamer-pro-policii-a-organycinne-v-trestnim-rizeni/.
28. ZOULOVÁ, Lenka a Miloslav FIŠER. Inteligentní kamery vidí i slyší. Chytré technologie mění česká města [online]. 2023 [cit. 2024-02-24]. Dostupné z:

https://www.novinky.cz/clanek/interneta-pc-inteligentni-kamery-vidi-i-slysi-chytre-technologie-meni-ceska-mesta-40450506.

Ostatní

1. Důvodová zpráva k zákonu 365/2011 Sb., kterým se mění zákon č. 262/2003 Sb., zákoník práce, ve znění pozdějších předpisů a dalších související zákony, bod 37.
2. EUROPEAN DATA PROTECTION BOARD. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky [online]. 2020. [cit. 2024-02-28]. Dostupné z: https://edpb.europa.eu/edpb_guidelines__video_devices_cs.pdf.
3. ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů [online]. 2024 [cit. 2024-02-24]. Dostupné z: https://uoou.gov.cz/media/profesional/met-kamerove-systemy-web-08022024.pdf.
4. ÚOOÚ. Provozování kamerového systému z hlediska zákona o ochraně osobních údajů [online]. 2006 [cit. 2024-02-28]. Dostupné z: https://www.smocr.cz/Shared/Clanky/7086/stanovisko-uoouc-1-2006.
5. ÚOOÚ. Provozování kamerových systémů: Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů [online]. [cit. 2024-02-24]. Dostupné z: http://www.promenybydleni.eu/metodika_provozovani_kamerovych_systemu.pdf
6. ÚOOÚ. Přepravní a dopravní společnost (UOOU-04151/20) [online]. 2021 [cit. 2024-03-19]. Dostupné z: https://uoou.gov.cz/cinnost/ochrana-osobnich-udaju/ukoncene-kontroly/kontroly-zarok-2021/kontrolni-cinnost-v-oblasti-ochrany-osobnich-udaju-2021/prepravni-a-dopravnispolecnost-uoou-0415120.
7. ÚOOÚ. Shrnutí Pokynů 3/2019 ke zpracování osobních údajů prostřednictvím videozařízení [online]. [cit. 2024-02-29]. Dostupné z: https://www.helpgdpr.cz/rstsp/clanky.nsf.pdf
8. ÚOOÚ. Umístění kamerových systémů v bytových domech [online]. 2016 [cit. 2024-02-28]. Dostupné z: https://www.scmbd.cz/UOOU_Umisteni_kamerovych_systemu_v_bytovych_domech.
9. ÚOOÚ. ÚOOÚ k biometrické identifikaci nežádoucích osob na fotbalových stadionech [online]. 2019 [cit. 2024-02-25]. Dostupné z:

https://m.uoou.cz/vismo/dokumenty2.asp?id=35541&n=uoouk-nbsp-biometricke-identifikaci-nezadoucich-osob-na-fotbalovych-stadionech.

10. ÚOOÚ. Výroční zpráva 2023 [online]. [cit. 2024-03-29]. Dostupné z: https://uoou.gov.cz/media/vyrocni-zpravy/vz2023-elektronicka-verze.pdf.
11. WP29. Stanovisko č. 2/2017 ke zpracování údajů na pracovišti. European Commisson [online]. 2017, [cit. 2024-03-18]. Dostupné z: https://ec.europa.eu/newsroom/article29/items/610169
12. WP29. Stanovisko č. 6 /2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. European Commisson [online]. 2014 [cit. 2024-03-18]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2014/wp217_cs.pdf