



Časté právní mýty o kamerách na pracovišti

Kamerové systémy patří mezi oblíbené nástroje ochrany majetku a bezpečnosti (nejen) na pracovištích. Zároveň však představují významný zásah do soukromí zaměstnanců i dalších osob. V praxi se stále setkáváme s řadou zjednodušujících představ a zažitých mýtů o tom, kdy je kamerový dohled „v souladu s právem“. Tento článek se zaměřuje na nejčastější omyly spojené s používáním kamer na pracovišti a ukazuje, že nejde pouze o otázku GDPR, jak se často zaměstnavatelé domnívají, ale o souběh pravidel více právních předpisů.

Shrnutí od AI

Článek je názorovým textem, který vyvrací šest rozšířených mýtů o právní regulaci kamerových systémů na pracovištích. Autorka zdůrazňuje, že zavádění kamerového systému nelze redukovat pouze na splnění požadavků GDPR, protože souběžně vstupují do hry zákoník práce a obecná ochrana osobnosti podle občanského zákoníku, přičemž ani souhlas zaměstnance ani ochrana majetku jako taková nezaručují automatickou přípustnost kamerového sledování. Upozorňuje rovněž na to, že i online kamerové systémy bez záznamu a atrapy kamer mohou za určitých okolností zakládat právní povinnosti nebo porušení práv zaměstnanců. Pro splnění informační povinnosti nestačí pouhá informační tabulka s piktogramem, ale je nezbytné zaměstnance prokazatelně a podrobně informovat, zpravidla prostřednictvím vnitřního předpisu. Praktický dopad článku umocňuje skutečnost, že Státní úřad inspekce práce zařadil kontroly kamerových systémů na pracovištích mezi své hlavní priority pro rok 2026, což zvyšuje riziko postihů pro zaměstnavatele, kteří právní rámec podceňují. [méně](#)

Kamery na pracovišti jsou často ze strany zaměstnavatelů vnímány jako opatření, které má pomoci zvýšit bezpečnost zaměstnanců, předejít krádežím, usnadnit řešení vzniklých škod nebo jinak ochránit majetek zaměstnavatele. V praxi se poměrně často setkáváme s rozsáhlým monitoringem pracovišť s využitím nejmodernějších kamerových systémů umožňujících zaznamenávat obraz i zvuk, avšak právní rovina používání těchto systémů bývá často upozaděna.

Kamerový systém se jeví jako rychlé, snadné a efektivní řešení mnoha problémů, kdy stačí pouze nakoupit kamery, vše správně připojit a je vyřešeno. Taková představa je však zjednodušená. Kamerový systém totiž nepředstavuje jen bezpečnostní prvek, ale také významný zásah do základních práv fyzických osob. Používání kamerového systému na pracovišti má proto svá pravidla, která je třeba při zavádění kamerového systému respektovat a zamýšlené řešení jim přizpůsobit. A právě v tomto bodě vzniká řada mýtů, které bych tímto článkem ráda objasnila.

Mýtus 1: „Stačí splnit GDPR a je hotovo“

Jedním z nejrozšířenějších mýtů o používání kamerových systémů na pracovištích je přesvědčení, že kamerový systém je čistě otázkou ochrany osobních údajů a stačí proto naplnit požadavky vyplývající zejm. z GDPR.

GDPR je bezesporu důležitým právním předpisem, pokud jde o používání kamerových systémů na pracovištích, ale zdaleka není jediným. Na pracovišti vstupuje do hry zejména zákoník práce, který výrazně omezuje možnosti kontroly zaměstnanců, a rovněž obecná ochrana osobnosti podle občanského zákoníku.

Zaměstnavatel se tak může dostat do situace, kdy sice splní veškeré požadavky GDPR, ale samotné umístění kamer bude nepřípustné z hlediska pracovního práva. Kamera na pracovišti proto vždy vyžaduje komplexní posouzení, nikoli izolované „GDPR řešení“.

Mýtus 2: „Kamery máme jen online, GDPR se nás netýká“

Úřad pro ochranu osobních údajů („ÚOOÚ“) dříve ve své výkladové praxi zastával názor, že sledování osob prostřednictvím online kamery bez ukládání záznamu nepředstavuje zpracování osobních údajů a jako takové tedy nespadá pod GDPR. Tento výklad byl však ze strany ÚOOÚ zejména po vydání pokynů Evropského sboru pro ochranu osobních údajů („EDPB“) ke zpracování osobních údajů prostřednictvím videotechniky v roce 2020[1] revidován a v současné době již neobstojí.

Podle aktuálního výkladu EDPB i ÚOOÚ není pro aplikaci GDPR na kamerový systém rozhodující samotná existence záznamu, ale schopnost identifikovat fyzickou osobu. Jak výslovně uvádí ÚOOÚ[2], i online kamerové systémy mohou představovat zpracování osobních údajů.

Z právního hlediska navíc nelze přehlížet ani obecnou ochranu osobnosti a soukromí osob. Už samotná možnost být sledován může představovat zásah do těchto základních práv člověka, a to bez ohledu na to, zda je obrazový záznam uchováván. Stejně tak v případě pravidel pro sledování zaměstnanců na pracovišti podle zákoníku práce není rozhodné, zda je kamerový systém provozován v režimu online nebo se záznamem.

I v případě online kamerového systému je proto třeba respektovat obecná pravidla týkající se ochrany osobnosti, jakož i specifická pravidla na ochranu osobních údajů vyplývající zejm. z GDPR i specifická pravidla sledování zaměstnanců vyplývající ze zákoníku práce.

Mýtus 3: „Používáme jen atrapy, právní pravidla řešit nemusíme“

Atrapy kamer bývají ze strany zaměstnavatelů v praxi považovány za „bezpečnou“ variantu, která se právní regulací zcela vyhne, avšak může alespoň částečně umožnit dosažení stejného efektu jako kamera pravá, pokud nikdo neví, že jde o atrapu.

Ani zde však situace není tak jednoduchá. Pokud se nejedná o funkční kamerový systém, ale o atrapu, pohybuje se zaměstnavatel skutečně mimo režim zpracování osobních údajů a pravidel GDPR. To ovšem neznamená, že taková atrapa je automaticky bezproblémová.

V určitých případech může i atrapa vyvolávat dojem trvalého sledování, který se negativně promítá do soukromí a psychické pohody zaměstnanců. Zaměstnavatel se proto takovým postupem může dopustit porušení svých povinností vyplývajících ze zákoníku práce, konkrétně povinnosti „vytvářet příznivé pracovní podmínky a zajišťovat bezpečnost a ochranu zdraví při práci“.

Mýtus 4: „Máme souhlas zaměstnance, můžeme kamery používat“

Souhlas zaměstnance bývá často vnímán jako „univerzální pojistka“, pokud jde o zpracování osobních údajů zaměstnanců (nejen) kamerovým systémem. V pracovněprávních vztazích je však použití souhlasu značně problematické. Zaměstnanec se nachází v podřízeném

postavení a jeho souhlas proto v praxi často nelze považovat za skutečně svobodný. Navíc je třeba mít na paměti, že souhlas může subjekt údajů kdykoliv odvolat, což v případě kamerových systémů nebude příliš praktické.

V praxi to tedy znamená, že zaměstnavatel by se měl opírat o jiný právní základ zpracování osobních údajů, typicky o oprávněný zájem. Ten však musí být vždy pečlivě posouzen a vyvážen s ohledem na práva zaměstnanců a s přihlédnutím ke konkrétním okolnostem daného případu.

Souhlas zaměstnance zároveň nenahradí ani splnění předpokladů vyplývajících pro sledování zaměstnanců kamerovým systémem ze zákoníku práce. Zákoník práce je v tomto ohledu poměrně striktní a pro možnost sledování zaměstnanců prostřednictvím kamerového systému vyžaduje, aby byl u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. Souhlasem zaměstnance proto tuto podmínku nelze splnit.

Mýtus 5: „Když kamera chrání majetek, je automaticky oprávněná“

Ochrana majetku zaměstnavatele je legitimním cílem, nikoli však automatickým ospravedlněním kamerového systému na pracovišti. Právní předpisy vyžadují, aby zaměstnavatel prokázal vždy nezbytnost a přiměřenost tohoto opatření. Nestačí proto tvrdit, že kamera chrání majetek, tudíž je oprávněná, ale je třeba vždy zkoumat, zda nebylo možné zvolit méně invazivní řešení a brát ohled na zaměstnance, kteří mají právo na určitou míru soukromí na pracovišti.

Zpracování osobních údajů je třeba vždy založit na jednom z právních základů dle GDPR, přičemž tím nejčastějším v případě kamerového systému bude ochrana oprávněných zájmů správce nebo třetí osoby. S tím však souvisí povinnost před zavedením kamerového systému provést tzv. balanční test, v němž se mimo jiné poměřuje zájem zaměstnavatele na ochraně majetku s právem zaměstnanců na soukromí. Bez tohoto kroku se přitom kamerový systém snadno může dostat do rozporu s právními předpisy.

Rovněž z pohledu zákoníku práce nestačí jako zdůvodnění uvést, že kamerami je chráněn majetek zaměstnavatele, ale musí být vždy zkoumána přiměřenost takového opatření s ohledem na soukromí zaměstnanců, stejně jako existence závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele, dochází-li prostřednictvím kamerového systému ke sledování zaměstnanců.

Mýtus 6: „Stačí cedulka s piktogramem a nápisem, že je prostor monitorován“

Viditelná informační cedulka s piktogramem kamery je důležitá, ale sama o sobě k naplnění informační povinnosti podle GDPR ani zákoníku práce nestačí.

GDPR stanoví poměrně rozsáhlý výčet informací, které je třeba subjektu údajů poskytnout. V případě kamerových systémů je proto doporučováno tzv. vícevrstvé informování, kdy první vrstvu informací představuje informační tabulka, kde však pouhý piktogram kamery není dostačující^[3]. Subjekt údajů musí mít k dispozici i podrobnější informace v rámci tzv. druhé vrstvy. Druhá vrstva má typicky podobu podrobnější informace v textové podobě, kterou lze vystavit na webu, zaslat, zapůjčit na požádání k prostudování apod.

Zákoník práce ukládá zaměstnavateli povinnost přímo informovat zaměstnance o rozsahu a způsobech monitorování. Pouhá tabulka na zdi přitom tento požadavek nenaplnuje. Každého zaměstnance je třeba podrobně a prokazatelně informovat o účelu, rozsahu a způsobu provádění sledování kamerovým systémem, např. prostřednictvím vnitřního předpisu.

Závěr

Kamerový systém na pracovišti nelze z právního pohledu považovat za jednoduché ani univerzální bezpečnostní řešení. Jde o citlivý zásah do práv zaměstnanců, který vyžaduje pečlivé právní posouzení s ohledem na konkrétní podmínky daného pracoviště a musí obstát současně z pohledu pracovního práva, ochrany osobnosti i ochrany osobních údajů.

Potřebu důkladného přístupu v této oblasti přitom umocňuje i skutečnost, že Státní úřad inspekce práce ve svém programu kontrol pro rok 2026^[4] výslovně deklaruje jako jednu z hlavních priorit právě kontroly zaměřené na používání kamerových systémů na pracovištích. Včasné a správné nastavení kamerového systému tak může zaměstnavatelům pomoci předejít nejen zásahům do práv zaměstnanců, ale i případným nepříjemným důsledkům kontrolní činnosti.



Mgr. Dominika Valentová,
advokátka

[Doležal & Partners s.r.o., advokátní kancelář](#)

Růžová 1416/17, 110 00, Praha 1

Koliště 1912/13, 602 00, Brno

Tel.: +420 222 544 201

e-mail: office@dolezalpartners.com

[1] EDPB. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky. Verze 2.0. Přijato dne 29. ledna 2020. Dostupné >>> [zde](#).

[2] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů. 2024. Dostupné >>> [zde](#).

[3] Tabulka by měla obsahovat piktogram/obrázek kamery, údaj o tom, že prostor je monitorován kamerovým systémem, identifikaci správce a odkaz na kontaktní osobu, odkaz na místo, kde je možné získat podrobnější informaci, účel a právní základ zpracování osobních údajů a informace o právech subjektu údajů.

[4] SÚIP. Program kontrolních akcí Státního úřadu inspekce práce na rok 2026. Dostupné >>> [zde](#).