SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

MONITORING ZAMĚSTNANCŮ – ROZVOLNĚNÍ/ÚPRAVA PRAVIDEL V SOULADU S LIMITY DLE EVROPSKÉ LEGISLATIVY (A V SOULADU S EVROPSKOU JUDIKATUROU)

FORLEX s.r.o., advokátní kancelář

MONITORING ZAMĚSTNANCŮ – ROZVOLNĚNÍ/ÚPRAVA PRAVIDEL V SOULADU S LIMITY DLE EVROPSKÉ LEGISLATIVY (A V SOULADU S EVROPSKOU JUDIKATUROU

Ostrava
2024

AUTORSKÝ KOLEKTIV

Mgr. Pavel Říha, advokát a společník

Mgr. Simona Zahradníčková, trvale spolupracující advokátka

Mgr. Kamila Fišerová Ulrichová, trvale spolupracující advokátka

Mgr. Štěpánka Kočařová, advokátní koncipient

Mgr. David Juchelka, advokátní koncipient

SEZNAM POUŽITÝCH ZKRATEK

ČR	Česká republika
ESLP	Evropský soud pro liská práva
LZPEU	Listina základních práv Evropské unie
LZPS	Listina základních práv a svobod ČR
NS	Nejvyšší soud
NSS	Nejvyšší správní soud
OZ	zákon č. 89/2012 Sb., občanský zákoník
SDEU	Soudní dvůr Evropské unie
SFEU	Smlouva o fungování Evropské unie
TZ	zákon č. 40/2009 Sb., trestní zákoník
ÚOOÚ	Úřad pro ochranu osobních údajů
ÚS	Ústavní soud ČR
WP29	Pracovní skupina pro ochranu údajů zřízená podle čl. 29
ZP	Zákon č. 262/2006 Sb., zákoník práce

Obsah

1. ÚVOD

Monitoring zaměstnanců je v poslední době čím dál častěji celospolečenským tématem. Zejména po covidové pandemii zaznamenáváme v některých skupinách populace nevoli přijmout jakoukoliv formu sledování na pracovišti či mimo něj. Monitoring zaměstnanců existoval již dávno před vypuknutím pandemie a v zásadě jej zaměstnanci dokázali přijmout a pochopit jeho účel. Ne vždy však zaměstnavatelé nastavují kontrolu na pracovišti správně a v těchto případech mohou být oprávněné obavy zaměstnanců z dopadu takového monitoringu na jejich soukromí a ochranu jejich osobních údajů.

Současná česká právní úprava řeší monitoring zaměstnanců jen okrajově. Striktně formální výklad dotčených ustanovení zákoníku práce může mít za následek téměř nemožnost efektivního využití monitoringu zaměstnanců. Řada zaměstnavatelů naopak přistupuje k monitorování svých zaměstnanců, aniž by důsledně vyhodnotila zákonné požadavky, neboť se domnívá, že ochrana majetku zaměstnavatele je v pracovněprávních vztazích prioritou.

Vzhledem k tomu, že oblast monitorování zaměstnanců není na úrovni Evropské unie jednotná, s výjimkou ochrany osobních údajů, může český zákonodárce hledat inspiraci pro zkvalitnění českého právního prostředí v oblasti monitoringu zaměstnanců v zahraničí. Jednotlivé státy Evropské unie volí různé přístupy, ať již přijetím specifických zákonů zabývajících se monitoringem zaměstnanců nebo volnější režim založený na obecných právních principech doplněný judikaturou. Důležitým podkladem pro formování právního prostředí v oblasti monitoringu zaměstnanců jsou také výkladová stanoviska, která v jednotlivých státech tvoří zejména autority pro oblast ochrany osobních údajů. Stanoviska nejvýznamnějších evropských úřadů na ochranu osobních údajů jsou často používána i v dalších státech Evropské unie.

Tento dokument si klade za cíl specifikovat, jaké formy monitoringu přicházejí v pracovněprávních vztazích v úvahu, popsat současný stav právní úpravy v oblasti monitoringu zaměstnanců v České republice, popsat a porovnat právní úpravy ve vybraných státech Evropské unie (tj. Finsko, Německo a Francie) a navrhnout, jak by se dál měla vyvíjet česká právní úprava, aby oblast monitoringu byla pro subjekty práva uživatelský příjemnější, a přitom zaručovala dostatečnou ochranu základních práv subjektů právní úpravy.

2. DEFINICE MONITORINGU ZAMĚSTNANCŮ

Česká právní úprava neobsahuje zákonnou definici monitoringu zaměstnanců na pracovišti. Obecně však monitoring můžeme označit za činnosti vykonávání dohledu zaměstnavatele na pracovišti, který umožňuje zaměstnavateli sledovat nebo zaznamenávat výkonnost, polohu, chování a osobní znaky zaměstnance v reálném čase, nebo jako součást širších organizačních procesů, jako je například testování na návykové látky.[1]

Monitoring zaměstnanců může být prováděn v reálném čase či zpětně (prostřednictvím záznamu o činnostech zaměstnance) prostřednictvím kamerových, zvukových a jiných záznamů, monitorovacího softwaru, GPS lokalizátorů a dalších zařízení.

[1] Ball, K. Workplace surveillance: an overview [online]. *researchgate.net*. [cit. 12. 9. 2024]. https://www.researchgate.net/publication/45229880_Workplace_Surveillance_An_Overview

3. PRÁVNÍ ÚPRAVA MONITORINGU ZAMĚSTNANCŮ V ČESKÉ A EU LEGISLATIVĚ

V České republice neexistuje zákon, který by se zabýval výhradně ochranou soukromí zaměstnanců na pracovišti, jako je tomu kupříkladu ve Finsku[2]. V českém právním řádu je problematika monitoringu zaměstnanců primárně upravena v ZP, který stanoví základní pravidla a východiska sledování zaměstnanců na pracovišti.

Problematickým aspektem monitoringu zaměstnanců je především konkurence základních práv a svobod zaměstnavatele a zaměstnance zakotvených v LZPS, které stojí proti sobě a navzájem kolidují. Na straně zaměstnance se jedná o právo na soukromí, které zaměstnanec požívá i na pracovišti, na straně zaměstnavatele se jedná o právo vlastnit a chránit svůj majetek. V kontextu monitoringu je tedy nutné zabývat se tím, zda v daném případě převáží právo na soukromí zaměstnance nad právem zaměstnavatele na vlastnictví a ochranu majetku zaměstnavatele či naopak. Takové porovnání se provádí zpravidla pomocí tzv. testu proporcionality, který stojí na třech kritériích: kritériu vhodnosti, potřebnosti (nutnosti) a poměřování. Výsledek testu proporcionality pak stanoví možnosti a mantinely monitoringu pro konkrétní případ.

Nelze také opomenout předpisy na úseku ochrany osobnosti a předpisy na ochranu osobních údajů, zejm. GDPR, které se sice nezabývá monitoringem jako takovým, ale nastavuje pravidla pro sběr, zpracování a uchování osobních údajů, ke kterému při monitoringu zaměstnanců zpravidla dochází.

Jednotlivým předpisům a jejich významu pro monitoring zaměstnanců se budeme věnovat v následujících podkapitolách.

3.1. Listina základních práv a svobod

LZPS, jak již vyplývá z jejího názvu, určuje základní okruh práv, která požívají zvýšené ochrany. Mezi těmito základními právy je i právo na nedotknutelnost osoby a soukromí, které je pro oblast monitoringu zaměstnanců klíčové, neboť právě to zamezuje zaměstnavateli v tom, aby zaměstnance podrobil monitoringu bez omezení. Toto právo je vymezeno v článcích 7 odst. 1, článku 12 a článku 13 LZPS.

[2] Act on Protection of Privacy in Working life 759/2004. Finsko.

Článek 7 odst. 1) LZPS

Čl. 7 odst. 1) LZPS stanoví, že nedotknutelnost osoby a jejího soukromí je zaručena a omezena může být jen v případech stanovených zákonem. Jedná se o základní pilíř práva na soukromí. Nejedná se však o právo absolutní, neboť je omezitelné zákonem.[3] Právo na soukromí je pak nejčastěji omezováno z důvodů ochrany práv a zájmů jiných osob. To platí i v pracovněprávních vztazích, ve kterých právo zaměstnance může být omezeno např. v situaci, určí-li tak zákon, nebo v situaci, kdy proti tomuto základnímu právu zaměstnance stojí základní právo zaměstnavatele například na ochranu majetku, které v daném konkrétním případě převyšuje nad zájmem zaměstnance.

Článek 10 odst. 2) LZPS

Článek 10 stanoví, že každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Právo na respektování soukromého a rodinného života je svou povahou velmi obsáhlé a zahrnuje ochranu před neoprávněnými zásahy do mnoha sfér privátní oblasti lidského života, konkrétní vymezení však LZPS neobsahuje a to proto, aby byla ochrana pružná a umožnovala vzít v úvahu sociální, právní i technické aspekty jednotlivých případů a zohlednit aktuální politické, sociální i kulturní stránky lidské společnosti. V kontextu monitorování zaměstnanců tak východiskem pro určení, co je a co není zásahem do soukromého a rodinného života bude relevantní judikatura českých soudů a Evropského soudu pro lidská práva.

Článek 11 odst. 1) LZPS

Článek 11 odst. 2) LZPS stanoví, že každý má právo vlastnit majetek. Vlastnické právo všech osob má stejný zákonný obsah a ochranu. Tento článek LZPS je základním stavebním prvkem pro právo zaměstnavatele chránit svůj majetek, a navazující oprávnění zakotvené v ZP provádět kontrolou využívání svěřených výrobních a pracovních prostředků zaměstnanci.

[3] Nechvátalová, L. Komentář: Listina základních práv a svobod, 1. vydání [online]. *beck-online.cz*. [cit. 12. 9. 2024]. https://app.beck-online.cz/bo/document-view.seam?documentId=nnptembsgfpwk232ge4texzrfzrwyny

Článek 12 LZPS

Článek 12 stanoví, že obydlí je nedotknutelné. Bez souhlasu toho, kdo v něm bydlí tedy do něj nelze vstoupit. V pracovněprávních vztazích však existují situace, kdy zaměstnavatel bude mít oprávněný zájem na tom, aby nahlédl, alespoň z části do obydlí zaměstnance, např. při výkonu zaměstnání zaměstnance na dálku tzv. „*home-office*“.[4], kdy zaměstnavatel může legitimně požadovat, aby si zaměstnanec zapnul kameru a mikrofon při konferenčním hovoru, dále zejména v oblasti prevence bezpečnosti a ochrany zdraví při práci.

Článek 13 LZPS

Článek 13 zavádí právo na ochranu listovního tajemství, tedy na ochranu soukromí při komunikaci skrze písemnosti a jiné záznamy. Do jisté míry tento článek konkretizuje obecnější právo na respektování soukromého a rodinného života. Do kolize s uvedeným právem zaměstnance se zaměstnavatel dostane zpravidla v situaci, kdy chce provádět kontrolu korespondence zaměstnance nehledě na to, zda se jedná o fyzickou poštu, e-mailovou nebo telefonickou komunikaci.[5]

3.2. Listina základních práv Evropské unie

Listina základních práv Evropské unie se ve velké míře překrývá s českou LZPS, proto na tomto místě nebudeme znovu uvádět výčet základních práv a svobod uvedených výše. Nad rámec již zmíněných základních práv a svobod však LZPEU navíc obsahuje pro monitoring relevantní právo na ochranu osobních údajů zakotvené v článku 8 LZPEU.

Článek 8 LZPEU

Článek 8 odst. 1) LZPEU zakládá právo každého na ochranu osobních údajů, které se jej týkají. Odst. 2) tohoto článku dále doplňuje, že osobní údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené

[4] Bočanová, V., Cibulková, M. Stanovisko CzELA k právním otázkám institutu home office – 8. část [online]. *epravo.cz*. [cit. 12. 9. 2024]. https://www.epravo.cz/top/clanky/stanovisko-czela-k-pravnim-otazkam-institutu-home-office-8-cast-112936.html

[5] Štefko, M. § 316 Majetek zaměstnavatele; soukromí zaměstnance; nesouvisející informace. In: Bělina, M., Drápal, L. a kol. *Komentář: Zákoník práce, 4. vydání*. Praha: C. H. Beck, 2023, s. 1397.

osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.

3.3. Smlouva o fungování Evropské unie

Článek 16 SFEU

Stejně jako v LZPEU, článek 16 SFEU v odst. 1) stanoví, že každý má právo na ochranu osobních údajů, které se jej týkají.

3.4. Občanský zákoník

OZ ochranu soukromí upravuje především v ustanovení § 86, ve kterém navazuje na základní práva obsažená v LZPS a tyto rozvádí a konkretizuje. Dle uvedeného ustanovení nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy. V citovaném paragrafu je znovu akcentována potřeba zákonného důvodu pro zásah do soukromí osoby.

Na uvedené ustanovení navazuje ustanovení § 88 odst. 1), dle kterého svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použije k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob. Toto ustanovení tedy zakládá právo zaměstnavatele monitorovat zaměstnance bez jejich souhlasu, pokud takový monitoring provádí v souvislosti s ochranou svých zájmů.

Ustanovení § 90 pak stanoví, že zákonný důvod k zásahu do soukromí jiného člověka nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka.

3.5. Zákoník práce

ZP je stěžejním zákonným předpisem obsahující právní úpravu monitoringu zaměstnanců na pracovišti, který obsahuje zákonnou výjimku, díky které je zaměstnavatel

v určitých případech oprávněn zasáhnout do soukromí zaměstnance. Tato výjimka je vymezena v ustanovení § 316 ZP v odstavcích 1, 2 a 3.

Dle ustanovení § 316 odst. 1) platí, že: „*Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.*“ Dle zákona tedy platí, že pokud zaměstnavatel výslovně neumožní užívání svěřených pracovních prostředků pro soukromé účely, jsou zaměstnanci povinni tyto prostředky využívat výhradně a pouze k plnění pracovních úkolů. Je pak přirozené, že zaměstnavatel musí mít možnost plnění této zákonné povinnosti zaměstnanců přiměřeným způsobem kontrolovat. Zákonné zmocnění zaměstnavatele ke kontrole je však třeba vyložit v souladu s principem nezbytnosti. Zaměstnavatel je tedy oprávněn provádět kontrolu, ale pouze v nezbytném rozsahu a přiměřeným způsobem. Legálnost kontroly tak závisí na tom, zda zvolený způsob kontroly a její provedení bude přiměřené všem okolnostem daného případu. V této souvislosti je nutné uvažovat zejména povahu a závažnost kontrolovaných povinností zaměstnance, závažnost chráněných zájmů zaměstnavatele, míru soukromí zaměstnance, která je narušena a existenci jiných, méně invazivních prostředků, kterými by bylo možné dosáhnout téhož výsledku.

Dle druhého odstavce platí, 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*.“

Druhý odstavec specifikuje okolnosti, za kterých je možné provádět kontrolu zaměstnance ze strany zaměstnavatele, pokud oprávnění ke kontrole nevychází přímo či nepřímo ze zákona. Nevyplývá-li tedy povinnost nebo právo realizovat kterýkoliv ze způsobů zásahu do soukromí zaměstnance, které jsou uvedeny v druhém odstavci (otevřené či skryté sledování, odposlech či kontrola komunikace) ze zvláštního právního předpisu, je možné takový zásah provádět pouze v případě, kdy zaměstnavatel má pro kontrolu závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele.

Ustanovení § 316 odst. 2 se vztahuje pouze na způsoby kontroly, které jsou v odstavci výslovně uvedené, tj. otevřené či skryté sledování, odposlech a záznam telefonických hovorů a kontrola elektronické pošty a listovních zásilek adresovaných zaměstnanci.

Dle ustanovení § 316 odst. 3) ZP platí následující: *„Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.“*

Dle odst. 3) je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění. Otázce, jakým způsobem a v jakém rozsahu musí zaměstnavatel zaměstnance o monitoringu informovat se budeme věnovat v dalších kapitolách.

I v případě že zaměstnavatel bude zaměstnance monitorovat v souladu se ZP, je zároveň nutné, aby splnil požadavky vyplývající pro zpracování osobních údajů podle GDPR.

3.6. GDPR

Nařízení Evropského parlamentu a Rady (EU) 2016/679 obecně známé pod zkratkou GDPR se sice nezaměřuje konkrétně na monitoring zaměstnanců, jedná se však o předpis obecně upravující sběr, zpracování a uchování osobních údajů, k čemuž při monitoringu zaměstnanců na pracovišti zpravidla dochází. Na monitoring zaměstnanců jakožto způsob zpracování osobních údajů lze tedy aplikovat obecné zásady zpracování obsažené v čl. 5 GDPR, které musí být naplněny, aby se nejednalo o protiprávní zpracovávání osobních údajů. Mezi tyto zásady patří především:

(a) zákonnost, korektnost, transparentnost;
(b) omezení účelu;
(c) minimalizace údajů;
(d) přesnost;
(e) omezení uložení;
(f) integrita a důvěrnost.[6]

[6] Ministerstvo vnitra ČR. Zásady zpracování osobních údajů [online]. *mvcr.cz.* [cit. 12. 9. 2024]. https://www.mvcr.cz/gdpr/clanek/zasady-zpracovani-osobnich-udaju.aspx

V případě, že by zaměstnavatel nedodržel nařízením požadované zásady, vystavuje se riziku sankce a povinnosti nahradit zaměstnanci újmu z toho vzniklou. Jak správně postupovat v souladu s GDPR v případně konkrétních činností zpracování osobních údajů stanoví také výkladový stanoviska a metodiky ÚOOÚ a dokumenty doporučující povahy zpracovávané Evropským sborem pro ochranu osobních údajů[7], mezi které patří např. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky.

3.7. Ostatní předpisy

Mezi další předpisy dopadající na monitoring zaměstnanců se řadí ZIP a TZ, které určují sankce, které mohou zaměstnavatele postihnout v případě, že zasáhne do soukromí zaměstnance mimo zákonem vymezené limity.

3.7.1. Zákon o inspekci práce

Zákon o inspekci práce svěřuje orgánům inspekce práce podle ustanovení § 11a a § 24a kontrolu a ukládání sankcí v souvislosti s porušením ustanovení § 316 ZP. Za porušení povinností plynoucích z ustanovení § 316 ZP hrozí FO nebo PO pokuta do výše 1.000.000 Kč, v případě, že naruší soukromí zaměstnance na pracovišti některým ze způsobů uvedených v ustanovení § 316 odst. 2) ZP, nebo pokuta do výše 100.000 Kč v případě, že zaměstnavatel neinformuje zaměstnance o rozsahu kontroly a způsobech jejího provádění podle ustanovení § 316 odst. 3) ZP. Dříve kontrolu nad dodržováním ustanovení § 316 ZP prováděl ÚOOÚ, tato kontrola však byla následně svěřena orgánům inspekce práce. To však nevylučuje, aby byla zaměstnavateli udělena pokuta ze strany ÚOOÚ v případě, že zaměstnavatel splní požadavky stanovené v ustanovení § 316 ZP bez toho, aniž by dodržel standard na zpracování osobních údajů daný GDPR.

3.7.2. Trestní zákoník

Nelze opomenout možnou trestněprávní rovinu nezákonného monitoringu zaměstnanců, kdy se zaměstnavatel může dopustit trestného činu.

[7] European Data Protection Board [online]. *edpb.europa.eu.* [cit. 12. 9. 2024]. https://www.edpb.europa.eu/our-work-tools/documents/our-documents_cs

§ 181 TZ

Poškození cizích práv

Základní skutková podstata vymezená v ustanovení § 181 TZ odst. 1) uvádí, že kdo jinému způsobí vážnou újmu na právech tím, že a) uvede někoho v omyl, nebo b) využije něčího omylu, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti. Na tento navazují odst. 2) a 3), ve kterých jsou vymezeny speciální skutkové podstaty. Naplnění této skutkové podstaty by teoreticky mohlo přijít v úvahu v situaci, kdy by zaměstnavatel např. podrobil zaměstnance neoprávněnému extenzivnímu monitoringu a současně zaměstnance ubezpečoval o tom, že jej monitoringu nepodrobuje.[8]

§ 182 TZ

Porušení tajemství dopravovaných zpráv

Podle ustanovení § 182 TZ, který v základní skutkové podstatě stanoví, že kdo úmyslně poruší tajemství a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením, b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo c) neveřejného přenosu dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková data, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.[9] Zaměstnavatel by měl při nakládání s korespondencí zaměstnance postupovat s dostatečnou obezřetností tak, aby nenaplnil některou z výše uvedených skutkových podstat.[10]

[8] Lojda, J. Poškození cizích práv v judikatuře nejvyššího soudu [online]. *epravo.cz.* [cit. 12. 9. 2024]. https://www.epravo.cz/top/clanky/poskozeni-cizich-prav-v-judikature-nejvyssiho-soudu-94868.html

[9] Šámal, P., Škvain, P. § 182 Porušení tajemství dopravovaných zpráv. In: Šámal, P. a kol. *Komentář: Trestní zákoník, 3. vydání*. Praha: C. H. Beck, 2023, s. 2285.

[10] Hanák, J., Pruška L. Právo zaměstnavatele na narušení listovního tajemství [online]. *pravniprostor.cz.* [cit. 12. 9. 2024]. https://www.pravniprostor.cz/clanky/pracovni-pravo/pravo-zamestnavatele-na-naruseni-listovniho-tajemstvi

§ 183 TZ

Porušení tajemství listin a jiných dokumentů uschovaných v soukromí

Dalším trestným činem, který by připadal v úvahu ve spojitosti s monitoringem zaměstnanců je porušení tajemství listin a jiných dokumentů uschovaných v soukromí. V odst. 1) ustanovení § 183 TZ je vymezena základní skutková podstata tak, že kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, dat uložených v počítačovém systému nebo na nosiči informací anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci.

4. NEDOSTATKY SOUČASNÉ PRÁVNÍ ÚPRAVY

Za hlavní nedostatek současné vnitrostátní právní úpravy považujeme její strohost, kdy celá problematika monitorování zaměstnanců na pracovišti je obsažena ve třech odstavcích ustanovení § 316 ZP. Uvedené ustanovení je zároveň poměrně vágní a obsahuje neurčité pojmy, které jsou těžko uchopitelné pro laickou, ale často i odbornou veřejnost. V praxi největší problém činí zřejmě posouzení toho, co je možné považovat za „*závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele*“. Některé výklady jsou více konzervativní a za zvláštní povahu činnosti zaměstnavatele považují například vysoko rizikové prostředí nebo pracovní prostředí, ve kterém se nakládá s vysokými hodnotami, dle jiných výkladů zvláštní povahou činnosti zaměstnavatele může být prakticky cokoliv, neboť v každém případě jde při provozování podnikání o ochranu majetku zaměstnavatele. Tyto nejasnosti činí právní úpravu pro zaměstnavatele velmi netransparentní a krajně problematickou, neboť nedává jasná pravidla a vodítka k posouzení toho, zda jimi zamýšlenou činnost sledování lze považovat za v souladu se zákonem či nikoliv, a zároveň zaměstnancům nenapovídá, jaké formy monitoringu jsou již excesivní a mohou se tedy dovolávat svých práv. Zaměstnavatelé se před přijetím opatření zavádějící monitoring důvodně obávají, že uvedený obecný zákaz monitoringu obsažený v první větě odstavce 2 je tak široký a neurčitý, že se vždy mohou najít argumenty, proč je uvažované opatření excesivní a v rozporu se zákonem.

Jediným vodítkem pro dovození zákonnosti konkrétního monitorovacího opatření je tak judikatura českých soudů, která však není příliš obsáhlá. Nedostatečnost, resp. neobsáhlost judikatury českých soudů v oblasti monitoringu může být důsledkem právě toho, že zaměstnavatelé ani zaměstnanci sami nejsou schopni posoudit svůj případný úspěch ve sporu o zákonnosti monitoringu, a proto se do sporu nepouštějí, případně zaměstnavatelé od zavedení opatření monitoringu zcela upustí, nebo provádí monitoring skrytě. Tím se problém dostává do kruhu, jehož výsledek jenom posiluje nejistotu zaměstnavatelů a zaměstnanců.

Zaměstnavatelé a zaměstnanci však nejsou jedinými, kdo tápe ve výkladu ustanovení § 316 ZP. Jasno nemají často ani příslušné úřady, které mohou ustanovení v důsledku vykládat pro jistotu více rigidně, než je zapotřebí nebo nekonzistentně.

Aktuální právní úprava v neposlední řadě neodpovídá a nestačí každodenní realitě zaměstnavatelů, zejména prudkému vývoji v oblasti technologií.

Důsledkem výše uvedených nedostatků české právní úpravy v oblasti monitoringu je tak situace, kdy zaměstnavatelé odrazeni neurčitostí právní úpravy buď upouští od zavedení efektivních sledovacích zařízeních na pracovišti, nebo v horším případě zavádí skryté formy sledování, které by jinak v otevřené formě a za zavedení příslušných ochranných opatření mohly být přijatelné a zcela v souladu se zákonem.

Jak přitom plyne ze srovnání s některými zahraničními systémy, právní úpravu monitoringu lze podchytit lépe, resp. přesněji, a tak oběma stranám vytvořit jistější limity toho, co ještě je či není dovoleno, a v důsledku tak zajistit lepší ochranu subjektivních práv zaměstnance na soukromí a zaměstnavatele na ochranu svého majetku.

5. PŘEDPOKLADY MONITORINGU ZAMĚSTNANCŮ

Předpoklady pro monitoring zaměstnanců lze tedy rozdělit do dvou rovin, a to na vyplívající z vnitrostátního práva a vyplývající z práva EU.

5.1. Vnitrostátní předpoklady

Vnitrostátní základ a předpoklady výkonu práva kontroly jsou, jak již bylo předestřeno výše, upraveny v ustanovení § 316 odst. 1) až 3) ZP. Ustanovení § 316 ZP je nutné vykládat komplexně.[11] Tím je myšleno, že v případě, že se zaměstnavatel rozhodne provádět kontrolu podle odst. 1) a zvolí některý prostředek monitoringu uvedený v odst. 2), musí naplnit předpoklady obou těchto paragrafů a informační povinnost uvedenou v odst. 3), aby bylo možné považovat provedený monitoring za zákonný. Naopak výlučně podle odst. 1) se bude postupovat pouze v případě, že zaměstnavatel využije prostředky kontroly, které nejsou vyjmenovány v odst. 2), tedy například nahlédnutí do knihy jízd služebního vozu, nebo jiná kontrola realizovaná v reálném čase, jde-li o ad hoc případy za účelem kontroly užívání svěřených výrobních a pracovních prostředků a v takovém případě nebude zaměstnavatel povinen zaměstnance o provedení kontroly informovat.[12][13]

Zároveň je zaměstnavatel povinen zavedení monitoringu zaměstnanců projednat s odborovou organizací v souladu s ustanovením § 287 odst. 2) písm. g) ZP, pokud by se monitoring týkal většího počtu zaměstnanců.

Pro zavedení monitoringu zaměstnanců musí existovat buď zákonný důvod nebo oprávněný zájem zaměstnavatele. Takovým oprávněných zájmem může být ochrana zdraví zaměstnavatele a jiných osob a ochrana majetku zaměstnavatele a jiných osob. Tento důvod pro zavedení monitoringu zaměstnavatele limituje v tom, jakým způsobem bude moci kontrolu provádět.

Kontrola musí být omezena na pracoviště, popřípadě pohyb mimo pracoviště v rámci výkonu práce, nesmí však být směřována na místa určená k hygieně nebo odpočinku zaměstnance.[14] V obydlí zaměstnance lze provádět kontrolu jen zcela výjimečně a ve velice

[11] Štefko. § 316: Majetek zaměstnavatele; soukromí zaměstnance; nesouvisející informace, s. 1397.
[12] Morávek J. Kontrola a sledování zaměstnanců – výklad § 316 ZPR. *Právní rozhledy.* 2017, č. 17, s. 573.
[13] Rozsudek Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011.
[14] Hůrka, P. § 316 Ochrana soukromí zaměstnance [online]. *ASPI*. [cit. 9. 6. 2024] Dostupné v Systému ASPI.

omezeném rozsahu, především pak při kontrole zaměstnance vykonávajícího práci z domova.

Zaměstnavatel je omezen také v předmětu sledování, tedy v tom, co přesně bude monitorovat, a to převážně právy zaměstnance. Rozsah sledovaných a zaznamenávaných informací tak není neomezený a zaměstnavatel vždy musí dbát na to, aby vymezil rozsah sledování v souladu se zákonem a s právy zaměstnance.

Dalším faktorem je způsob provedení sledovacích opatření. Zaměstnavatel je oprávněn provádět pouze otevřené sledování, tedy musí zaměstnance předem informovat o rozsahu kontroly a o způsobech jejího provádění. Z judikatury NS a ESLP však lze dovodit, že v určitých případech lze podrobit zaměstnance i skrytému sledování, a to především v případech, kdy by dokazovanou skutečnost nebylo možné prokázat jinak, např. v případech, kdy by skryté sledování prokázalo, že dochází k závažnému protiprávnímu jednání ze strany zaměstnance.[15]

Zaměstnavatel je však vždy povinen postupovat v souladu se zákonem tak, aby nebylo zasaženo do práv zaměstnanců, především tedy do práva na soukromí, nad zákonem povolenou míru. Naproti sobě tak stojí oprávněné zájmy zaměstnavatele a právo zaměstnance na soukromí.

5.1.1. Předpoklady pro monitoring zaměstnanců v kontextu užívání výrobních a pracovních prostředků zaměstnavatele

Pro kontrolu využívání výrobních a pracovních prostředků svěřených zaměstnanci je stěžejní odst. 1) ustanovení § 316 ZP. Podle toho je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat, jestli zaměstnanec používá jemu svěřené výrobní a pracovní prostředky v souladu s pracovní smlouvou, dalšími dohodami uzavřenými se zaměstnancem a vnitřními předpisy zaměstnavatele.

Prvním předpokladem je tedy svěření výrobních nebo pracovních prostředků zaměstnavatele zaměstnanci.

Druhým předpokladem je, že zaměstnavatel neudělil zaměstnanci souhlas s neomezeným využíváním svěřených prostředků pro osobní potřebu. Jak již bylo uvedeno výše, podle § 316 odst. 1) nesmí zaměstnanec užívat bez souhlasu zaměstnavatele svěřené

[15] Štefko. § 316: Majetek zaměstnavatele; soukromí zaměstnance; nesouvisející informace, s. 1397.

výrobní a pracovní prostředky pro osobní potřebu. Zaměstnavatel může zaměstnanci udělit souhlas s využíváním prostředků pro osobní potřebu, čímž dochází k prolomení zákonem stanoveného zákazu. Při kontrole je tedy nutné přihlížet k tomu, zda a v jakém rozsahu zaměstnavatel učinil souhlas s užíváním prostředků a případná kontrola pak může směřovat pouze na dodržování povinností, jež nebyly zaměstnavatelem vyloučeny nebo zmírněny.[16]

Třetím předpokladem je přiměřenost způsobu kontroly, kdy v případě, že by zaměstnavatel nedodržel požadavek přiměřenosti, jednalo by se o neoprávněný zásah do soukromí zaměstnance a zaměstnavatel by se vystavil riziku negativních následků popsaných výše. Požadavek přiměřenosti je v tomto případě neurčitý právní pojem a je tedy na každém zaměstnavateli, aby sám vyhodnotil, jaký způsob zásahu do soukromí zaměstnance zvolí, tak, aby jej bylo možné považovat za přiměřený. Přiměřenost zásahu lze nicméně odvodit ze závěru pomocného balančního testu, ve kterém se posuzuje vhodnost, přiměřenost a nezbytnost daného opatření. Příklad takového balančního testu zveřejnil ÚOOÚ v Metodice k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů z roku 2024, který bude podrobně rozebrán v podkapitole 4.3. Obecně však lze říci, že kontrola by měla směřovat výhradně k zjištění, zda zaměstnanec dodržuje svoje pracovněprávní povinnosti a neměla by nad míru přiměřenou danému cíli kontroly narušovat soukromí zaměstnance.[17]

5.1.2. Předpoklady pro monitoring zaměstnanců podle ustanovení § 316 odst. 2) a 3) ZP

V určitých případech se monitoring zaměstnanců řídí ustanovením § 316 odst. 2) ZP, dle kterého nelze bez vážného důvodu podrobit zaměstnance určitým formám monitoringu. Prvním ze dvou základních předpokladů pro monitoring zaměstnanců je závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. Zvláštní činnost zaměstnavatele pak nemusí nutně znamenat, že jde o činnost vysoce rizikovou či

[16] Rozsudek Nejvyššího soudu sp. zn. 21 Cdo 1771/2011.
[17] Tamtéž.

nebezpečnou. Budou-li dodrženy podmínky pro daný druh sledovacího opatření a bude-li dán závažný důvod může kontroly provádět prakticky každý zaměstnavatel.[18]

Druhým základním předpokladem je určitá forma monitoringu. Tyto jsou vyjmenovány v odst. 2) taxativně a jedná se o otevřené nebo skryté sledování, odposlech a záznam jeho telefonických hovorů, kontrolu elektronické pošty nebo kontrolu listovních zásilek adresovaných zaměstnanci.

Třetím základním předpokladem, plynoucím z odst. 3), je pak povinnost zaměstnavatele přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění. Informační povinnost je přitom praxi možné splnit několika způsoby. Prvním způsobem je inkorporace informační doložky do pracovní smlouvy zaměstnance. Tento způsob je však nepraktický, neboť, v případě, že by si strany definovaly, v jakém rozsahu bude monitoring prováděn v pracovní smlouvě, musely by strany při změně rozsahu nebo způsobu provádění monitoringu uzavírat dodatky k pracovním smlouvám, což by v případě společností s větším počtem zaměstnanců, nebo se zaměstnanci, kteří by odmítali podepsat dodatky k pracovním smlouvám, představovalo problém. Dalším způsobem je inkorporace do interních směrnic zaměstnavatele, jako např. pracovní řád.[19] Je na místě také zmínit, že v případě, kdy zaměstnanec udělí souhlas s monitoringem jednostranným prohlášením zaměstnance, nejedná se o automatické splnění informační povinnosti zaměstnavatele. Ten je i nadále povinen zaměstnance informovat o rozsahu a způsobu monitoringu,[20] a splnění této informační povinnosti je povinen odpovídajícím způsobem prokázat.

Bez naplnění těchto tří podmínek se tedy nemůže jednat o zákonný monitoring zaměstnanců podle odst. 2) a 3) a zaměstnavatel by mohl být sankciován za narušování soukromí svých zaměstnanců. Nezákonnost monitoringu však může mít dopady i na použitelnost monitoringem opatřených dat v soudních a jiných řízeních, kdy je např. možné odmítnout nezákonně opatřené záznamy jako důkazy právě proto, že byly opatřeny v rozporu se zákonem.[21] I v tomto případě je však nutné, aby zaměstnavatel volil

[18] Jelínek, T. § 316: Majetek zaměstnavatele, soukromí zaměstnance a informace nesouvisející s výkonem práce a se základním pracovněprávním poměrem. In: Valentová, K., Procházka, J. a kol. *Komentář: Zákoník práce, 2. vydání*. Praha: C. H. Beck, 2022, s. 1007.
[19] Konečná & Zacha. Monitorování zaměstnanců zaměstnavatelem [online]. *konecna-zacha.com*. [cit. 12. 9. 2024]. https://www.konecna-zacha.com/monitorovani-zamestnancu-zamestnavatelem/
[20] Papoušek, M. Monitoring a sledování zaměstnanců [online]. *epravo.cz.* [cit. 12. 9. 2024]. https://www.epravo.cz/top/clanky/monitoring-a-sledovani-zamestnancu-112902.html
[21] Rozsudek Nejvyššího soudu ze dne 21. 10. 1998, sp. zn. 21 Cdo 1009/98.

takové prostředky monitoringu, které nebudou přesmíru zasahovat do soukromí zaměstnance.

5.2. Předpoklady monitoringu zaměstnanců podle práva EU

5.2.1. Podle GDPR

V rámci EU není monitoring zaměstnanců specificky upraven, a je tak na každém členském státu, aby nastavil limity a podmínky, za kterých je zaměstnavatel oprávněn zaměstnance monitorovat. Důležitou roli však při monitoringu zaměstnanců hraje ochrana osobních údajů, která je v rámci Evropského hospodářství upravena stejným nařízením o ochraně osobních údajů (GDPR). V této souvislosti lze dovodit, že principy monitoringu v rámci EHP nebudou příliš odlišné.

Zákonnost, korektnost, transparentnost

Zákonnost zpracování osobních údajů je dána v případě, že je zpracování prováděno na základě jednoho ze zákonných důvodů zpracování uvedených v čl. 6 GDPR.

V zásadě může právní základ pro zpracování osobních údajů poskytovat kterýkoli z uvedených zákonných důvodů, nicméně na základě prvního zákonného důvodu, tj. souhlasu zaměstnance může zaměstnavatel zavést monitoring jen ve zcela výjimečných případech, neboť souhlas jakožto zákonný důvod pro zpracování osobních údajů, a zejména pak sledování, je poměrně problematický.

Souhlas se zpracováním osobních údajů musí být svobodný, konkrétní, informovaný a jednoznačný. Souhlas může představovat problém v případech, kdy je monitorován větší počet zaměstnanců, neboť zaměstnavatel musí k zavedení daného plošného opatření získat souhlas od každého ze zaměstnanců. S ohledem na skutečnost, že souhlas je možné navíc kdykoliv odvolat, je souhlas jakožto zákonný důvod velmi nestabilní a opatření postavené na souhlasu tedy neustále hrozí, že po odvolání souhlasu nebude nadále zákonné.

Souhlas jakožto zákonný důvod zpracování osobních údajů je zároveň problematický v pracovněprávních vztazích z toho důvodu, že mohou panovat důvodné pochybnosti o tom, že takový souhlas byl udělen svobodně, neboť pracovněprávní vztah je nerovným vztahem podřízenosti. Lze si tak představit situaci, kdy udělení souhlasu zaměstnance

se zpracováním osobních údajů (zde konkrétně s monitoringem) je motivováno spíše obavou zaměstnance z případných negativních důsledků na pracovní poměr, které by neudělení souhlasu mělo, než svobodnou vůlí zaměstnance po posouzení všech pro a proti. Souhlas udělený z obavy či jinak v tísni však nesplňuje podmínku svobodnosti, a bylo by tedy možné jej označit za neplatný.

Naopak mezi nejčastěji používané důvody zpracování pro zaměstnavatele bude patřit zákonný důvod pod písm. f), tj. oprávněný zájem, který převažuje nad zájmy, právy a svobodami subjektů.[22] Méně běžným, avšak možným důvodem pro zpracování osobních údajů souvisejících se zavedením sledovacího opatření může být splnění zákonné povinnosti (pokud zaměstnavateli některý zákonný předpis předepisuje, aby prováděl sledování určitého prostoru apod.) nebo splnění smluvní povinnosti.

Transparentností zpracování se rozumí přijmutí vhodných opatření správcem, aby poskytl subjektům údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a stručných jazykových prostředků, na žádost, informace, které se subjektu údajů týkají.

Dodržení zákonnosti a transparentnosti zpracování pak zakládají korektnost postupů vůči subjektu údajů.[23]

Omezení účelu

Zpracovatel je povinen osobní údaje shromažďovat pro určité a legitimní účely a osobní údaje nesmějí být zpracovávány s těmito účely neslučitelným způsobem. Z toho plyne, že zaměstnavatel nemůže použít zpracované osobní údaje zaměstnanců pro jiné účely, než které sám při zavedení monitoringu stanovil. Nelze tedy např. použít kamerový záznam sloužící k ochraně majetku zaměstnavatele před krádežemi jako podklad pro rozvázání pracovního poměru se zaměstnancem z důvodu neplnění jeho pracovních

[22] Evropský sbor pro ochranu osobních údajů. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky [online]. *edpb.europa.eu*. 29. 1. 2020, bod 16 [cit. 13. 9. 2024]. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf

[23] Evropská komise. Jaké údaje lze zpracovávat a za jakých podmínek? [online]. *commission.europa.eu*. [cit. 12. 9. 2024]. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/overview-principles/what-data-can-we-process-and-under-which-conditions_cs

povinností, neboť by se jednalo o zpracování v rozporu s účelem shromažďování osobních údajů.

Minimalizace údajů

Zaměstnavatel nesmí shromažďovat údaje o zaměstnanci v rozsahu větším, než je přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány. Pokud by zaměstnavatel shromažďoval údaje v širším rozsahu, než by bylo přiměřené a relevantní, nesplnil by požadavek přiměřenosti a vystavil by se riziku sankce. U kamerových systémů lze rozsah zpracovávaných údajů omezit např. počtem umístěných kamer, nastavením záběru kamer, režimem kamerového záběru (online, živý), dobou uchování kamerového záznamu, počtem osob, které mají ke kamerovému záznamu přístup nebo deaktivací některých funkcí kamer.

Přesnost, omezení uložení, integrita a důvěrnost

Osobní údaje musí být přesné, tedy musí odpovídat realitě a zaměstnavatel je zároveň povinen v případě nepřesností osobní údaje aktualizovat a zamezit jejich zpracování. Přesností se může myslet např. v rámci použití kamerových systémů to, že zaměstnavatel zamezí neautorizovaným změnám záznamů, především sestřihům, vymazání části záznamu, nebo zásahu do technických prostředků. Zároveň je také nutné, pokud má záznam sloužit k případné identifikaci osob, aby kvalita záznamu byla dostatečná pro identifikaci osob.

Osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány.

Integrita a důvěrnost směřuje na technické a organizační zabezpečení osobních údajů.

Informační povinnost

Jedním z nejzásadnějších předpokladů pro zákonné zpracování osobních údajů (a tedy potažmo monitoring) je splnění informační povinnosti vůči subjektům osobních údajů (zaměstnancům). Zaměstnavatel v pozici správce osobních údajů je dle GDPR povinen poskytnout zaměstnancům informace o tom, jakým způsobem budou jejich osobní údaje, získané v souvislosti s prováděním sledování, zpracovány, a to stručným,

transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků.

Informační povinnost je nutné splnit nejpozději k okamžiku získání osobních údajů, vhodnější je však zaměstnance informovat předem. Mezi poskytované informace patří údaj o totožnosti a kontaktní údaje zaměstnavatele, kontaktní údaje případného pověřence pro ochranu osobních údajů, údaj o účelu zpracování a právním základu pro zpracování, případné příjemce nebo kategorie příjemců osobních údajů a případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci. Je-li to nezbytné pro zajištění spravedlivého a transparentního zpracování, je správce osobních údajů povinen poskytnout také další údaje jako například doba, po kterou budou osobní údaje uloženy.

S informační povinností zaměstnavatele je spojeno právo zaměstnance na přístup k osobním údajů. Zaměstnanec má právo získat od zaměstnavatele potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k informacím stanoveným v čl. 15 GDPR, jako např. účely zpracování, kategorie dotčených osobních údajů apod. Potvrzení zaměstnavatel vydává na základě žádost zaměstnance, a to bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádost, přičemž tuto lhůtu lze v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další dva měsíce.

Metodika obecného posouzení vlivu na ochranu osobních údajů 2020

Tento dokument vydaný ÚOOÚ slouží jako vodítko ke splnění povinnosti vypracovat obecné posouzení vlivu na ochranu osobních údajů plynoucí z GDPR čl. 35 a na ně navazující seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů.

Stanovisko č. 2/2017 ke zpracování osobních údajů

V tomto dokumentu se WP29 zabývá zpracováním osobních údajů na pracovišti a mimo jiné obsahuje postup při zpracování testu proporcionality v souvislosti s posouzením, zda je zamýšlené opatření sledování přiměřené daným okolnostem či nikoliv. Zaměstnavatel by měl dle stanoviska zvážit zejména, zda:

- je uvažovaná činnosti sledování nezbytná, a pokud ano, na základě kterého zákonného důvodu by ke zpracování osobních údajů (sledování) docházelo;
- navrhované zpracování osobních údajů je z pohledu zaměstnanců korektní, tj. zda zejména zaměstnanec může rozumně očekávat takové sledování v dané situaci;
- zpracování osobních údajů je proporcionální vzhledem k vyjádřeným obavám; a
- je zpracování osobních údajů transparentní.

6. FORMY MONITORINGU ZAMĚSTNANCŮ A STANOVISKA ÚOOÚ

Monitoring zaměstnanců lze vykonávat různými způsoby, mezi které se řadí kontrola výrobních a pracovních prostředků poskytnutých zaměstnavatelem zaměstnanci, kontrola pošty zaměstnance ať již fyzické, nebo elektronické, pořizování záznamů z pracoviště, snímání polohy zaměstnance prostřednictvím GPS a další. Monitoring zaměstnanců může být zaměřen na několik různých oblastí, a to především, zda plní zaměstnanec v pracovní době svoje pracovní povinnosti řádně a včas, zda neužívá zařízení zaměstnavatele pro svoji osobní potřebu nebo na monitoring na základě závažného důvodu spočívajícím ve zvláštní povaze činnosti zaměstnavatele. U všech těchto oblastí je však nutné, aby byly monitorovány na základě výše uvedených předpokladů tak, aby byl monitoring v souladu se zákonem.

ÚOOÚ se dlouhodobě zabývá monitoringem zaměstnanců, z pohledu zpracování osobních údajů, a k jednotlivým formám monitoringu publikuje stanoviska a metodiky, prostřednictvím kterých se snaží informovat veřejnost o tom, jak provádět monitoring v souladu se všemi potřebnými předpisy. Mezi tyto patří Stanovisko č. 1/2006, Stanovisko č. 2/2009, Stanovisko č. 6/2009, Stanovisko č. 2/2017, Metodika k provozování kamerových systémů 2012, metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů z roku 2024. Na poli EU vydává k problematice ochrany osobních údajů metodiky a stanoviska EDPB, který po účinnosti GDPR nahradila WP29, která vydala např. metodiku obecného posouzení vlivu na ochranu osobních údajů. Tyto stanoviska a metodiky nejsou právně závazné a je tak na zaměstnavateli, zda bude postupovat v souladu s těmito dokumenty, či nikoli. Obecně se však postupování podle metodik a stanovisek zaměstnavatelům doporučuje, neboť právě ÚOOÚ provádí kontrolu dodržování zákona při sběru a zpracování osobních údajů.

Soudy se stejně tak jako ÚOOÚ věnovaly otázkám týkajících se monitoringu zaměstnanců ve značné míře jak na evropské úrovni, tak v ČR. U jednotlivých forem monitoringu proto uvedeme jednotlivá relevantní rozhodnutí a jejich vliv na danou formu monitoringu zaměstnanců. Rozhodnutí ESLP a SDEU hrají v oblasti monitoringu zaměstnanců významnou roli, avšak při jejich posuzování je nutné pamatovat na to, že konkrétní

rozhodnutí jsou založená také na právní úpravě monitoringu jednotlivých států a není tedy možné aplikovat všechna rozhodnutí v ČR bez dalšího.

6.1. Kontrola zařízení

Počítač a obdobná zařízení jsou častými pracovními prostředky, které mohou být zaměstnanci ze strany zaměstnavatele poskytnuty k výkonu práce. Tato zařízení lze konkrétně sledovat několika způsoby:

- kontrolou aktivity na internetu;
- kontrolou souborů obsažených v zařízení;
- kontrolou aktivity na zařízení pomocí monitorovacího softwaru.

Z judikatury NS vyplývá, že zaměstnavatel je ke **kontrole aktivity na internetu** oprávněn, pokud zkoumá, zda zaměstnanec nevyužívá svěřená zařízení k osobním potřebám podle odst. 1) ustanovení § 316 ZP nebo zda využívá pracovní dobu efektivně k plnění pracovních povinností. Je však nutné, aby se zaměstnavatel při této kontrole omezil na zkoumání, zda dochází k neoprávněnému užívání a zdržel se zkoumání obsahu navštěvovaných stránek, aby nebylo nepřiměřeně zasaženo do soukromí zaměstnance. Zaměstnavateli lze doporučit, aby výslovně zakázal zaměstnancům používání internetu na pracovišti pro osobní účely. Kontrolu toho, zda zaměstnanec využívá efektivně pracovní dobu k plnění pracovních povinností by však měl být oprávněn provést i bez výslovného zákazu.

Jedním z možných způsobů, jak efektivně zamezit využívání svěřených pracovních prostředků k osobním účelům bez nutnosti zavedení sledování je zavedení tzv. blacklistů (tj. zakázaných webových stránek, které zaměstnancům nepůjdou na daném zařízení zobrazit) a whitelistů (tj. tedy seznamů povolených webových stránek, které lze na daném zařízení zobrazit). Takové řešení nicméně bude možné pouze v některých případech; v dnešní době se jedná spíše o přežitek.

Z judikatury NS vyplývá, že pokud zaměstnavatel provádí kontrolu jiným způsobem, než uvedeným v odst. 2) ustanovení § 316 ZP, nemusí být o kontrole zaměstnanec předem informován. Z uvedeného by bylo možné dovodit, že v případě, kdy je kontrola prováděna podle ustanovení 2 ustanovení § 316, není nutné o takové kontrole informovat;

to však platí pouze o ZP, avšak dle GDPR je nutné informovat o zpracování osobních údajů, zaměstnavatel se tedy splnění informační povinnosti nevyhne.

Co se týká **kontroly souborů v zařízení** je situace obdobná jako u předchozích situací. Kontrolovat soubory na zařízení může zaměstnavatel v případě, že chce ověřit, jestli zaměstnanec nevyužívá zařízení v rozporu se svými povinnostmi souvisejícími s pracovním poměrem nebo v rozporu se zákonem (např. zda nepoužívá software, který porušuje autorská práva jiné osoby). I v tomto případě je však nutné zachovat přiměřenost a zjišťování obsahu souborů, stejně jako zjišťování obsahu korespondence se považuje za nepřiměřené, ledaže je to nutné k naplnění stanoveného účelu. Zaměstnavatel tak při podezření ze zneužívání zařízení může kontrolovat, jaké soubory má zaměstnanec na zařízení uložené, ve většině případů však nesmí kontrolovat jejich obsah. V případě, že by soubory obsahovaly informace k jejichž přístupu by měl zaměstnavatel oprávněný zájem, mohl by do obsahu souborů nahlédnout.

Nejvyšší míru zásahu do soukromí zaměstnance pak představuje **kontrola aktivity pomocí monitorovacího softwaru** tzv. keyloggerů, který dovoluje zaměstnavateli sledovat veškerou aktivitu zaměstnance na zařízení. Tento způsob monitoringu lze považovat za excesivní i v případě existence závažného důvodu na straně zaměstnavatele. I v případě, že by závažný důvod existoval, pravděpodobně by bylo takové opatření vyhodnoceno jako nepřiměřené, pokud by zaměstnavatel mohl dosáhnout požadovaného účelu monitoringu i jiným způsobem.[24]

Kontrole zařízení svěřeného zaměstnanci se věnuje také judikatura ESLP a NS.

Rozsudek č. č. 588/13 ze dne 22. 2. 2018

Libert proti Francii

V tomto rozsudku se ESLP zabýval situací, kdy zaměstnavatel prozkoumal obsah souborů na zařízení zaměstnance, na základě čehož byl se zaměstnancem rozvázán pracovní poměr. Soud neshledal porušení práva na respektování soukromého a rodinného života, neboť francouzská legislativa výslovně umožňovala zaměstnavateli otevírat soubory související s výkonem zaměstnání a zaměstnanec v tomto případě neoznačil

[24] Pracovní skupina WP 29. Stanovisko č. 2/2017 ke zpracování osobních údajů na pracovišti (kapitola 5.4.1) [online]. *CODEXIS.* [cit. 6. 5. 2024] https://next.codexis.cz/literatura/LT111929

soubory jako soukromé, tudíž zaměstnavatel oprávněně předpokládal, že se jedná o soubory související s výkonem zaměstnání.

Z tohoto rozhodnutí plyne, že pokud legislativa umožňuje otevírání souborů zaměstnanců souvisejících s výkonem práce a zaměstnanec nerozliší soukromé soubory od pracovních, může zaměstnavatel soubory prohlédnout a případně vyvodit důsledky, pokud zjistí porušení zaměstnancových povinností. Toto rozhodnutí samo o sobě nelze aplikovat na českou právní úpravu, neboť základem pro kontrolu obsahu souborů na zařízení zaměstnance byla francouzská právní úprava, je však ukázkou toho, jak by potenciálně mohla vypadat úprava monitoringu zaměstnanců, pokud by došlo k legislativní změně.

Rozsudek NS č. 21 Cdo 1771/2011 ze dne 16. 8 .2012

Kasalova pila

V tomto rozsudku populárně známém jako Kasalova pila se NS zabýval věcí, ve které byl se zaměstnancem rozvázán pracovní poměr na základě kontroly zařízení, v souladu s ustanovením § 316 odst. 1 ZP, ze které vyplynulo, že zaměstnanec v rámci jednoho měsíce strávil v pracovní době přes sto hodin neefektivní prací na počítači. Zaměstnanec se domáhal neplatnosti zrušení pracovního poměru s tím, že jej zaměstnavatel neinformoval o kontrole internetových stránek v souladu s odst. 3) § 316 ZP a podrobil jej tak skrytému sledování. ÚS konstatoval, že zaměstnavatel se nedopustil nezákonného provedení kontroly, neboť prováděl kontrolu podle § 316 odst. 1) ZP a zároveň se nejednalo o kontrolu spadající pod odst. 2) a z toho důvodu nebyl zaměstnavatel podle odst. 3) povinen informovat zaměstnance o provádění kontroly. Soud řešil také otázku přiměřenosti kontroly ve vztahu k zásahu do soukromí zaměstnance a došel k závěru, že o soukromí zaměstnance jistě vypovídá, které internetové stránky zaměstnanec sleduje, avšak toto nebylo podstatou kontroly, přičemž zaměstnavatel nesledoval obsah navštěvovaných stránek. Podstatou kontroly bylo pouze zjistit, zda zaměstnanec sleduje stránky, které nesouvisí s výkonem zaměstnání, a tudíž byla míra zásahu do soukromí zaměstnance minimální a v souladu s odst. 1).

Z tohoto rozhodnutí tedy plyne, že zaměstnavatel je oprávněn kontrolovat, využívání svěřených výrobních a pracovních prostředků i když jednáním zaměstnance v rozporu se ZP nedochází ke škodě nebo ke snižování hodnoty svěřených zařízeních, ale kontrola je převážně prováděna za účelem zjištění porušování pravidel zacházení se svěřenými

prostředky v kontextu výkonnosti zaměstnance. Dále také plyne, že zaměstnavatel není povinen o kontrole podle odst. 1) § 316 zaměstnance předem informovat.

6.2. Telefon

Telefonní zařízení je dalším z pracovních prostředků, které mohou být zaměstnanci ze strany zaměstnavatele poskytnuty k výkonu práce. Na monitorování telefonu zaměstnance se vztahují v zásadě stejná pravidla, jako na ostatní zařízení, popsaná výše s tím, že u telefonu lze navíc monitorovat hovory, SMS a jiné obdobné krátké zprávy odeslané ze zařízení. Všechny tyto uvedené však podléhají listovnímu tajemství podle čl. 13 LZPS a zaměstnavatel by ve většině případů neměl zkoumat jejich obsah, pokud jsou adresovány přímo zaměstnanci. Odposlech a zaznamenávání telefonních hovorů je forma monitoringu zaměstnanců, která je přímo uvedena v odst. 2) § 316 ZP a zaměstnavatel je k tomuto monitoringu oprávněn pouze v případě, že existuje závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, a zároveň zaměstnance o monitoringu předem informuje. Nejčastějším případem monitorování telefonu je nahrávání hovorů v callcentrech, kdy je monitorována komunikace zaměstnance s klientem a tyto záznamy jsou využívány jako důkazy při uzavírání smluv se zákazníky, jako podklady ke zlepšení služeb nebo jako záznamní materiál řešení krizové situace za asistence operátora. V takovýchto případech se zpravidla jedná o monitoring, který spočívá v závažném důvodu spočívajícím ve zvláštní povaze činnosti zaměstnavatele.[25][26] V souvislosti se služebním telefonem může zaměstnavatel také kontrolovat statistické přehledy o hovorech a SMS, které obdrží od mobilního operátora, neboť tyto jsou dostatečně zobecněny na to, aby se nejednalo o nepřiměřený zásah do soukromí zaměstnance.[27] V tomto případě by se mohlo jednat o kontrolu podle odst. 1) § 316 ZP, neboť nedochází k odposlechu nebo záznamům telefonních hovorů a zaměstnanec tak o této kontrole nemusí být předem informován. Zaměstnavatel by v souladu s metodikou 5/2013 ÚOOÚ neměl v případě monitoringu za účelem zlepšování služeb uchovávat nahrávky déle než jeden měsíc. V případě zaznamenání

[25] Vidrna, J., Koudelka, Z. 2 Oprávněnost a neoprávněnost monitoringu. In: Vidrna, J., Koudelka, Z. *Zaměstnanci v objektivu kamer, 1. vydání.* Praha: C. H. Beck, 2013, s. 100.
[26] Úřad pro ochranu osobních údajů. Stanovisko č. 5/2013 Věstníku Úřadu pro ochranu osobních údajů [online]. *CODEXIS*. [cit. 5. 6. 20] https://next.codexis.cz/literatura/LT79916
[27] Papoušek. Monitoring zaměstnanců.

uzavření smlouvy pak lze předpokládat, že legitimní důvod uchování nahrávky bude trvat, dokud nebude smlouva mezi zaměstnavatelem a klientem naplněna.

Rozsudek NS č. 21 Cdo 1009/98 ze dne 21. 10. 1998

V tomto rozhodnutí se NS zabýval případem, kdy byl zaměstnanec propuštěn z důvodu plánovaného převzetí zákazníků zaměstnavatele, což zaměstnavatel dokládal nahrávkou telefonického hovoru mezi zaměstnanci. ÚS konstatuje, že zprávy podávané telefonem mezi zaměstnanci mohou být v souladu s čl. 13 LZPS korespondencí na kterou se vztahuje listovní tajemství. Zaměstnavatel tak není oprávněn tyto hovory zaznamenávat bez předchozího souhlasu nebo alespoň vyrozumění zaměstnanců. Dále ÚS konstatoval, že důkazy pořízené v rozporu s právními předpisy, tedy i záznam telefonního hovoru pořízený bez vědomí zúčastněných osob, nelze provést kvůli jeho nepřípustnosti.

Toto rozhodnutí ÚS bylo vydáno ještě za platnosti starého ZP, i přes to jsou však závěry v něm obsažené aktuální, především tedy závěr, že telefonní hovory podléhají listovnímu tajemství a pořizování jejich záznamů bez předchozího vyrozumění zaměstnance je v rozporu se zákonem.

Rozsudek NS 21 Cdo 747/2013 ze dne 7. 8. 2014

V tomto případě se jedná o obdobnou situaci jako v předchozím rozhodnutí Rozsudek NS Kasalova pila, kdy zaměstnavatel kontroloval, zda zaměstnanec nepoužívá služební počítač a telefon pro osobní potřebu. Nejvyšší soud vyvodil, že je nutné posuzovat, zda zaměstnavatel kontroloval hovory zaměstnance za účelem zjištění jejich obsahu, nebo aby zjistil, zda zaměstnanec používá zařízení pro osobní potřebu. V případě, že kontroloval způsob využití zařízení svěřených zaměstnanci, jedná se o kontrolu podle odst. 1) § 316 ZP. Zaměstnanec také poukazoval na to, že služební telefon mu byl předán již před nástupem do práce, NS však neshledal, že by den nástupu do práce hrát roli vůči možnosti používání svěřeného zařízení neměl a zaměstnavatel je oprávněn kontrolovat využití zařízení i před nástupem do práce.

6.3. Listovní zásilky

Listovní zásilky podléhají listovnímu tajemství zakotveném v čl. 13 LZPS. Zaměstnavatel by se tak měl zdržet otevírání a kontrolování soukromé pošty zaměstnance i když bude doručena na pracoviště. Je však nutné rozlišovat alespoň tři situace a to, zda je listovní zásilka určena přímo zaměstnanci bez provázanosti s jeho zaměstnáním, zda je určena zaměstnanci v rámci výkonu jeho zaměstnání, nebo zda je určena zaměstnavateli a zaměstnanec je pouze kontaktní osobou, která je oprávněna zásilku převzít. To lze rozlišovat primárně podle toho, jak je daná listovní zásilka nadepsaná.

V případě zásilky, která je adresována zaměstnanci bez připojení firmy podnikatele lze předpokládat, že se jedná o zásilku nesouvisející se zaměstnáním, a zaměstnavatel by se měl zdržet kontroly obsahu takovýchto zásilek, aby nedošlo k porušení listovního tajemství. Je však přípustné kontrolovat např. jejich četnost.

V případě zásilky, která je určena zaměstnanci v rámci výkonu jeho povolání by se měl zaměstnavatel uchýlit ke kontrole obsahu zásilky pouze ve výjimečných situacích, jako např. když je zaměstnanec dlouhodobě nemocný a zásilka obsahuje informace nezbytné pro ochranu zájmů zaměstnavatele. O této kontrole by však měl být zaměstnanec v souladu s odst. 3) § 316 ZP předem informován.

V případě, že je zaměstnanec pouze kontaktní osobou zaměstnavatele, nebo je jeho jméno na dopise zmíněno pro urychlení komunikace se zaměstnavatelem, je obsah korespondence určen primárně zaměstnavateli a ten by měl mít možnost seznámit se obsahem zásilky bez toho, aniž by se jednalo o monitoring zaměstnance.

6.4. E-mailová a jiná elektronická komunikace

E-mailová a jiná elektronická komunikace, například skrze platformy jako WhatsApp, Facebook Messenger atd., požívá stejně jako listovní zásilky listovního tajemství podle čl. 13 LZPS. Kontrola jejich obsahu tak spadá pod odst. 2) § 316 ZP a o kontrole je zaměstnavatel povinen zaměstnance informovat. Zaměstnavatel však smí monitorovat primárně kvantitu komunikace nebo velikost obsahu přijaté a odeslané komunikace, Velikost obsahuje odesílaných zpráv je zpravidla monitorována z různých i bezpečnostních důvodů, např. v rámci kontroly, zda komunikace neobsahuje nebezpečné viry, nebo za účelem ochrany před přetížením serverů. V případě, že vznikne podezření

ze zneužití pracovních prostředků, smí zaměstnavatel kontrolovat taktéž předmět a hlavičku, tj. odesílatele a adresáty korespondence. Další situací, kdy může zaměstnavatel kontrolovat komunikaci zaměstnance na základě ochrany svých zájmu jsou v případy, kdy je zaměstnanec dlouhodobě pracovně nedostupný např. z důvodu nemoci, jedná se o na první pohled pracovní komunikaci a je nutné ji otevřít, aby nebylo zasaženo do oprávněných zájmů zaměstnavatele.[28] V rámci posouzení přiměřenost zavedení sledovacího opatření, resp. přistoupení k otevření e-mailu a jiných zpráv zaměstnance se nicméně vždy přihlíží ke všem okolnostem případu; zaměstnavatel by v této souvislosti měl prokázat, že učinil jiná nezbytná opatření k dosažení uvažovaného cíle, které však nebyly v dané situaci efektivní, například se pokusil s nepřítomným zaměstnancem spojit mimo práci, nebo ve vnitřním předpise stanovil zaměstnancům povinnost vždy před dlouhodobější nepřítomností v práci přesměrovat všechny příchozí e-maily na jiného zaměstnance tak, aby byla zajištěna kontinuita práce.

Stanovisko ÚOOÚ č. 2/2009 aktualizované v únoru 2014

V tomto stanovisku se ÚOOÚ věnoval rozlišení soukromé a pracovní pošty a použití soukromé a pracovní e-mailové adresy. U fyzické pošty je zásadní samotná obálka, kdy u soukromé zásilky je jméno a příjmení zaměstnance uvedeno na prvním místě a název zaměstnavatele slouží především jako adresní údaj. Na druhou stranu, pokud je zásilka nadepsána na prvním místě firmou zaměstnavatele, bude se pravděpodobně jednat o poštu určenou zaměstnavateli, i když bude zaměstnanec na zásilce nadepsán jako kontaktní osoba. U e-mailové komunikace je nutné rozlišovat především osobní e-mail svěřený zaměstnanci v rámci výkonu jeho zaměstnání a úřední e-mail, který zaměstnanec pouze spravuje pro zaměstnavatele. Pokud je e-mail zřízen na některém z free-mailových serverů, jako např. google.com nebo seznam.cz, jedná se vždy o osobní e-mail zaměstnance.

Dále se v tomto stanovisku ÚOOÚ věnoval zacházení se zaměstnanci v souvislosti s monitoringem. ÚOOÚ shrnul zákonem stanovené podmínky, které musí zaměstnavatel vůči zaměstnanci dodržovat. Podmínka číslo 1. není sice již aplikovatelná,

[28] Úřad pro ochranu osobních údajů. Stanovisko č. 2/2009 Věstníku Úřadu pro ochranu osobních údajů [online]. *CODEXIS*. [cit. 5. 6. 20] https://next.codexis.cz/literatura/LT12650

přesto podmínky 2. a 3. lze vztáhnout na monitoring podle aktuální právní úpravy. Jsou jimi:

1. informovat zaměstnance podle § 11 zákona o ochraně osobních údajů a § 30 a 31 nového zákoníku práce. V případě monitorování zaměstnanců při používání internetu je součástí informace vysvětlení principů monitorování jako je například soubor logů apod.;
2. se všemi zaměstnanci zacházet rovně; a
3. vycházet ze skutečného stavu. Byť zákon umožňuje, aby zaměstnancům byly některé činnosti zaměstnavatelem zakázány, zaměstnavatelem stanovená pravidla by měla odrážet realitu, tj. nezakazovat něco, co je u zaměstnavatele běžnou tolerovanou praxí.[29]

Rozsudek velkého senátu č. 61496/08 ze dne 5. 9. 2017

Bărbulescu proti Rumunsku

V tomto rozhodnutí se ESLP věnoval případu, kdy zaměstnavatel požádal zaměstnance, aby založil účet na Yahoo Messenger, aby mohl odpovídat na žádosti zákazníků. Z vnitřních předpisů zaměstnavatele plynulo, že zaměstnanci nejsou oprávněni používat zařízení společnosti k soukromým účelům. Zaměstnavatel provedl kontrolu zařízení zaměstnance v celkové délce osmi dnů bez toho, aniž by zaměstnance dopředu informoval o provedení kontroly. Zaměstnanec byl o kontrole informován následně s tím, že ze záznamu vyplývá, že zařízení používá pro soukromé účely a zaměstnanec byl následně propuštěn. Zaměstnanec se proti zrušení pracovního poměru bránil a vnitrostátní soudy rozhodly, že nahlédnutí do komunikace zaměstnance byl jediný způsob, jak ověřit, zda nepoužívá zařízení v rozporu s vnitřními předpisy. V této věci byly vydány dva rozsudky, kdy v prvním ze dne 12. 1. 2016 ESLP shledal, že nebylo zasaženo do zaměstnancova práva na respektování soukromého a rodinného života. Rozhodnutí bylo založeno na tom, že zaměstnavatel neměl podezření o porušování vnitřních předpisů a pouze si chtěl ověřit, že se tak neděje a také to, že zaměstnavatel má právo kontrolovat, zda zaměstnanec v pracovní době plní své pracovní povinnosti. Dalším důvodem bylo, že se monitoring nezabýval obsahem komunikace a monitoring se omezil pouze

[29] Úřad pro ochranu osobních údajů. Stanovisko č. 2/2009 Věstníku Úřadu pro ochranu osobních údajů [online]. *CODEXIS*. [cit. 5. 6. 20] https://next.codexis.cz/literatura/LT12650

na uvedený účet a nezabýval se dalšími daty v počítači. Ve výše nadepsaném rozsudku pak velký senát ESLP shledal, že do práva zaměstnance na respektování soukromého a rodinného života přeci jen zasaženo bylo, když zaměstnavatel zaměstnance předem neinformoval o tom, že jeho komunikace může být monitorována a také proto, že byla zaměstnanci udělena nejpřísnější sankce, tedy rozvázání pracovního poměru.

Z tohoto rozhodnutí je tedy patrné, že neinformuje-li zaměstnavatel zaměstnance o provedení kontroly v rozporu se zákonem, dojde k porušení práva na soukromí zaměstnance.

6.5. Kamery na pracovišti

Kamery jsou jedním z nejčastějších způsobů monitoringu zaměstnanců, a i proto se jejich úpravě více věnuje i samotný ÚOOÚ. Kamery na pracovišti mohou představovat zásah do soukromí většího okruhu zaměstnanců než výše zmíněné formy monitoringu, což je jeden z důvodů, proč by zavedení kamer nemělo být první volbou zaměstnavatele při ochraně jeho zájmů, který by měl hledat jiný způsob monitoringu, který by do práv zaměstnanců zasahoval méně. Takovým způsobem může být například kontrola vedoucím zaměstnancem nebo alarm.[30]

Sledování skrze kamerové systémy ať už živý přenos, nebo pořizování záznamu, spadá pod odst. 2) § 316 ZP, je možné jej zavést pouze na základě závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele, a je nutné zaměstnance o tomto způsobu monitoringu předem informovat. Povinnost informovat zaměstnance předem plyne z judikatury ESLP, kdy v případě, že zaměstnavatel zaměstnance neinformuje o monitoringu, bude záznam pořízen v rozporu se zákonem a nebude moct být použit jako důkaz před soudem.

Jak jsme již výše uváděli, výklad neurčitého pojmu „závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele“ činí v praxi potíže. Obecně se však za legitimní důvod zavedení kamerového systému považuje ochrana majetku zaměstnavatele, kdy jsou kamery umístěny zejména u vchodů/vjezdů do budovy a dalších důležitých místech (sklad, pokladna apod.), důvodným však v některých případech může být i umístění kamer po celém prostoru pracoviště zaměstnavatele (vyjma šaten, toalet

[30] Gembalová. K. Jak používat kamery na pracovišti [online]. *pravniprostor.cz.* [cit. 12. 9. 2024]. https://www.pravniprostor.cz/clanky/ostatni-pravo/jak-pouzivat-kamery-na-pracovisti

a odpočinkové místnosti). Obecně je dále zaměstnavatelům doporučováno neumisťovat kamery tak, aby nepřetržitě snímaly stálé pracoviště zaměstnance, neboť to by mohlo v nepřiměřené míře narušovat zaměstnancovo soukromí. I z toho pravidla si lze představit výjimky v případech, kdy to vyžadují okolnosti případu.

Dalšími důvody pro zavedení kamerového systému na pracovišti může být například sledování výroby a zdokonalování technologického postupu. Takové kamerové systémy nejsou zpravidla určeny k monitorování osob, avšak nelze vyloučit, že příležitostně se zaměstnanci do záběru dostanou, popř. pouze část těla zaměstnance (ruce, pokud kamera snímá výrobní linku). Na tyto situace je nutné myslet a zaměstnancům v této souvislosti poskytnout odpovídající ochranu, je-li to nezbytné k zajištění odpovídající míry soukromí.

Pokud by zaměstnavatel zvažoval instalaci atrap kamer, nemusí plnit zákonné povinnosti kladené na monitoring zaměstnanců, neboť k žádnému reálnému monitoringu nedochází. Měl by však mít na paměti, že i přes to, že nedochází ke zpracování osobních údajů a nehrozí mu sankce ze strany ÚOOÚ, je možné, aby mu sankce přeci jen udělena byla, a to ze strany inspekce práce, neboť zaměstnavatel má zákonnou povinnost vytvářet zaměstnancům příznivé pracovní prostředí a instalace atrap kamer by mohla být v rozporu s touto povinností.[31][32]

Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů z roku 2024

Tato metodika navázala na metodiku z roku 2012, kterou však rozšířila především o vzorové dokumenty, jako informační dokument pro subjekty údajů, záznam o činnosti zpracování osobních údajů, nebo o bilanční test, pomocí kterého by měl zaměstnavatel být schopen posoudit, zda jeho vybrané řešení nezasahuje do soukromí zaměstnance nepřiměřeným způsobem.

Tento test se skládá z několika kroků a to:

1. Posouzení dosažení účelu jinými prostředky (kritérium potřebnosti)

[31] Gembalová. Jak používat kamery na pracovišti.
[32] Protokol o kontrole Úřadu pro ochranu osobníc údajů ze dne 14. 4. 2021, čj. UOOU_04151/20-16.

2. Posouzení nezbytnosti zpracování osobních údajů v rámci vybraného řešení pro zajištění správcem definovaných účelů (kritérium vhodnosti)
3. Posouzení přiměřenosti zpracování osobních údajů (kritérium poměřování)

Tyto kroky je nutné vyhodnocovat postupně a pokud zaměstnavatel, byť v jednom bodě shledá, že nebylo naplněno uvedené kritérium, měl by od zavádění monitoringu pomocí kamerového systému upustit. Pokud zaměstnavatel vyhodnotí, že jím zvolený způsob monitoringu splňuje všechna tři kritéria, měl by tento způsob zásahu být v souladu se zákonem.

ÚOOÚ dále uvádí, že zaměstnavatel by měl vypracovat technický popis kamerového systému, popsat stupeň identifikace osob na kamerovém záznamu a zpracovat popis operací zpracování. Podle této metodiky je zaměstnavatel oprávněn kamerové záznamy uchovávat maximálně po 72 hodin a pokud by se rozhodl pro uchování delší, musí tak učinit na základě oprávněného důvodu, jako např. použití záznamu v trestním řízení.

Rozsudek velkého senátu č. 1874/13 ze dne 17. 10. 2019

López Ribalda a ostatní proti Španělsku

V tomto rozsudku řešil ESLP, zda bylo zasaženo do práva na respektování soukromého života stěžovatelek tím, že jim byla dána výpověď na základě kamerového záznamu, který byl pořízen v rozporu se zákonem. Zaměstnavatel v této věci pojal podezření, že stěžovatelky, které byly zaměstnány jako prodavačky, kradou zboží a rozhodl se nainstalovat kamery, které byly zaměřeny na stěžovatelky tak, aby bylo možné opatřit důkazy o jejich protiprávním jednání. Zákon však vyžadoval, aby o monitoringu zaměstnavatel zaměstnance informoval, což se nestalo. Zaměstnavatel skutečně opatřil kamerové záznamy, na kterých byly stěžovatelky při krádežích zachyceny a stěžovatelkám byla dána výpověď z disciplinárních důvodů. Případ se dostal až k ESLP a ten shledal, že došlo k porušení práva stěžovatelek na respektování soukromého života, neboť monitoring probíhal po delší dobu, stěžovatelky nebyly informovány a ochrana zájmů zaměstnavatele mohla být alespoň do určité míry zabezpečena jinak, zejména právě samotným informováním stěžovatelek o zavedení monitoringu, čímž by pravděpodobně došlo ke snížení četnosti krádeží. Naopak použití kamerového záznamu jako důkazu v soudních řízeních o ukončení pracovního poměru nepovažoval za porušení práva

na spravedlivý proces, neboť vnitrostátní soudy se ve svých rozhodnutích opřely o vícero důkazů a řízení jako celek tak bylo možné označit za spravedlivé.

Z tohoto rozsudku tedy vyplývá, že neinformuje-li zaměstnavatel zaměstnance v souladu se zákonným požadavkem o rozsahu a způsobu monitoringu, zasáhne do práva na respektování soukromého života zaměstnance a pokud by byl záznam použit jako jediný důkaz pro rozvázání pracovního poměru před soudy, a soud by na základě tohoto potvrdil rozvázání pracovního poměru, došlo by i k porušení práva na spravedlivý proces zaměstnance.

Nález ÚS II. ÚS 2806/08 ze dne 27. 1. 2010

Ke vztahu odposlechů v trestním řízení a práva na soukromí

V tomto nálezu ÚS posuzoval případ, kdy byli trestně stíháni zaměstnanci Městského úřadu v Rychnově nad Kněžnou, kteří byli v rámci vyšetřování podrobeni skrytému sledování. Soudy prvního stupně tvrdily, že záznamy nebyly pořízeny podle §88 trestního řádu, ale jako záznamy dokumentující dění ve veřejném prostoru, k jejichž pořízení nebylo třeba nařízení předsedou senátu. Dále také tvrdili, že zaměstnancům úřadů jakožto vykonavatelům veřejné moci nenáleží na pracovišti právo na soukromí. S tímto se ztotožnil také odvolací soud. ÚS oproti tomu konstatoval, že i kdyby bylo možné souhlasit s tím, že kancelář, ve které je vykonávána veřejná moc je veřejným prostorem, automaticky z toho nelze vyvozovat, že by kdokoliv na místě výkonu státní služby postrádal soukromí. Právo na soukromí v takových případech může být velice omezené, nemůže však být neexistující, neboť pak by mohl být zaměstnanec podroben v podstatě neomezené kontrole.

Z tohoto nálezu tedy plyne, že zaměstnanec má právo na soukromí vždy, otázkou však je, do jaké míry je omezeno okolnostmi.

Rozsudek NSS 10 As 245/2016-41 ze dne 20. 12. 2017

V tomto rozsudku NSS zkoumal situaci, kdy zaměstnavatel provozující autobusovou dopravu zavedl kamerový monitoring v autobusech za účelem ochrany majetku zaměstnavatele, zaměstnanců a přepravovaných osob. Kamera byla zaměřena výlučně na řidiče autobusu a stevarda a záznam měl být uchován po pět až devět dní. NSS uvedl, že pouze z povahy provozování autobusové přepravy nelze předpokládat výrazně zvýšené

riziko, pro které by bylo nezbytné zavádět monitoring. NSS také uvedl, že zaměstnavatel mohl využít i jiných prostředků pro ochranu majetku osob. NSS se ve své argumentaci odkázal na princip proporcionality, kdy je nutné zkoumat vůči sobě jednotlivá práva a posoudit které z nich převáží. NSS uzavřel, že sice bylo naplněno kritérium vhodnosti, nebylo však naplněno kritérium potřebnosti, a proto označil kasační stížnost za nedůvodnou.

Z tohoto rozhodnutí tedy plyne, že na monitoring zaměstnanců je nutné uplatnit princip proporcionality a v případě, že převáží sledovaný chráněný zájem zaměstnavatele nad soukromím zaměstnance, lze zavést přiměřené opatření k jeho ochraně.

6.6. GPS

K zavedení monitoringu pomocí GPS, dochází především v situacích, kdy zaměstnavatel chce kontrolovat zaměstnance, který vykonává práci mimo prostory zaměstnavatele. Pokud by zaměstnavatel chtěl kontrolovat zaměstnance v rámci svých prostor, pravděpodobně by se jednalo o nepřiměřený způsob kontroly, neboť si lze představit způsoby kontroly, které méně zasahují do soukromí zaměstnance, jako např. kontrola vedoucím zaměstnancem.

Tento způsob monitoringu tedy může sloužit k několika různým účelům, mezi které se řadí kontrola najetých kilometrů služebním vozem, kontrola efektivity zaměstnance např. při doručování zásilek, nebo kontrola, zda zaměstnanec v pracovní době vykonává práci. Pomocí GPS může zaměstnavatel nahlížet také do soukromí zaměstnance mimo pracovní dobu, zejména díky tomu, že GPS může snímat polohu služebního vozu nepřetržitě po celý den. GPS má tedy z pohledu kontroly zaměstnance velký potenciál pro zasahování do soukromí zaměstnance a je důležité, aby zaměstnavatel přesně vymezil účely, pro které monitoring pomocí GPS zavádí a aby se zdržel opatřování a využívání dat mimo rámec vymezeného účelu. Z judikatury ESLP vyplývá, že přiměřeným zásahem do soukromí zaměstnance je zkoumání najetých kilometrů u služebního vozu svěřeného zaměstnanci s tím, že jej může používat i pro osobní účely, pokud je zaměstnanec kupříkladu povinen platit náhradu za opotřebení na základě najetých kilometrů a údaje jsou nutné k vyúčtování náhrad. V takovém případě totiž zaměstnavatel zkoumá pouze výši najetých kilometrů a nezkoumá např. k jakým cestám zaměstnavatel služební vůz využil Nepřiměřeným zásahem by naopak bylo dlouhodobé zkoumání toho, kdy byl

služební vůz nastartován a parkován, za účelem kontroly dodržování pracovní doby ze strany zaměstnance. Takováto kontrola by byla potenciálně přípustná, pokud by zaměstnavatel prováděl namátkové kontroly zaměstnanců v omezeném časovém období a sledoval by pouze údaje v rozmezí pracovní doby tak, aby nezasahoval do soukromí zaměstnance. I v takovém případě si však lze přestavit, že by zaměstnavatel mohl využít i jiných prostředků, jak zjistit, zda zaměstnanec pracovní dobu dodržuje.

Důležitá je také otázka zpracování osobních údajů. Pokud lze na základě dat z GPS v kombinaci s přístupem do jiných databází identifikovat zaměstnance, jedná se o zpracování osobních údajů i v případě, že zaměstnavatel k identifikaci zaměstnanců data z GPS nepoužívá. V takovém případě je pak nutné dodržet všechny předpoklady stanovené GDPR. Zároveň by také zaměstnavatel měl provést test proporcionality vzhledem ke zvolenému opatření a posoudit, zda je způsob sběru dat přiměřený. K účelu, pro který je sběr prováděn.

Rozsudek číslo č. 26968/16ze dne 13. 12. 2022

Florindo de Almeida Vasconcelos Gramaxo proti Portugalsku

V tomto rozsudku se ESLP zabýval případem, kdy zaměstnavatel umístil do služebního vozu poskytnutého zaměstnanci GPS lokalizátor za účelem přesného výpočtu náhrady náležející zaměstnavateli za opotřebení automobilu v případě, že zaměstnanec používá služební automobil pro osobní účely. Proti zaměstnanci bylo zahájeno disciplinární řízení z důvodu nadhodnocování počtů kilometrů v rámci plnění svých pracovních povinností, nedodržování pracovní doby a nedovoleného manipulování se zařízením. Zaměstnanec byl propuštěn a proti tomuto se bránil žalobou. Odvolací soud rozhodl, že do práva na soukromý život zaměstnance bylo zasaženo jen sledováním nastartování a parkování vozidla, z čehož bylo dovozeno nedodržování pracovní doby, neboť tím zaměstnavatel sledoval zaměstnance nad přiměřenou míru. O monitorování najetých kilometru však rozhodl, že to nepředstavuje zásah do soukromí zaměstnance, neboť je nezbytně nutné pro vyčíslení náhrady. S tímto závěrem se ztotožnil i ESLP, který konstatoval, že odvolací soud svým rozhodnutím nezasáhl do práva na soukromí zaměstnance, když považoval měření najetých kilometrů za oprávněné.

Z tohoto rozhodnutí tedy plyne, že je-li to nezbytné, např. pro posouzení nákladů na provoz automobilu nebo případné náhrady za jeho používání, může zaměstnavatel GPS

do automobilu umístit. Zaměstnavatel by se však měl vyvarovat extensivnímu monitorování zaměstnance, především pak mimo pracovní dobu tím, že by GPS byla aktivní nepřetržitě.

Rozsudek Městského soudu v Praze č. 6 A 42/2013-48 ze dne 5. 5. 2017

V tomto případě se žalobce Česká pošta domáhal zrušení rozhodnutí ÚOOÚ týkajícího se používání GPS lokalizátorů pro sledování pohybu zaměstnanců. ÚOOÚ rozhodl o tom, že žalobce zpracovává osobní údaje, když lze potenciálně propojit údaje o poloze jednotlivých pracovníků s rozpisem služeb. Cílem nasazení GPS bylo získání statistických dat o obslužnosti adresných bodů, jímž mělo být docíleno zrychlení a zkvalitnění služeb. I v tomto případě soud provedl test proporcionality, ze kterého vyplynulo, že rozsah kontroly byl nepřiměřený sledovaným účelům a že žalobce měl zvážit jiné alternativy.

6.7. Monitorování biometrických údajů

Podle čl. 9 odst. 1) GDPR je mimo jiné zakázáno zpracovávání biometrických údajů za účelem jedinečné identifikace fyzické osoby, neboť tyto spadají do zvláštní kategorie osobních údajů. Z tohoto zákazu jsou v odst. 2) dány výjimky, obecně však lze říct, že by se zaměstnavatelé měli zdržet zavádění zařízení pro čtení biometrických údajů sloužících např. pro vstup na pracoviště, neboť k naplnění tohoto účelu jistě existují i jiné dostatečné prostředky. V případě zavedení zařízení pro čtení biometrických údajů by zaměstnavatel měl na zvolené opatření aplikovat test proporcionality, aby vyhodnotil, zda je zavedení opatření oprávněné. V určitých případech je však představitelné, že by zařízení pro čtení biometrických údajů obstála bez větších potíží, a to především v zařízeních, na jejichž ochraně má zájem široká veřejnost, jako jsou např. vojenská zařízení, jaderné elektrárny, nebo banky, neboť tato zařízení vyžadují vyšší míru zabezpečení. Naproti tomu si lze představit, že budou zařízení pro čtení biometrických údajů nainstalována např. pro vstup zaměstnanců do zaměstnání v případě, že se jiná opatření v minulosti ukázala jako neefektivní k naplnění požadovaného účelu a využití biometriky je tedy jediným efektivním řešením v souvislosti se všemi okolnostmi dané

situace. Obecně však platí, že monitoring zaměstnance za pomoci zařízení pro čtení biometrických údajů by byl s největší pravděpodobností považován za nepřiměřený.[33]

6.8. Jiné typy monitoringu zaměstnanců

Mimo výše uvedené však existují i další způsoby monitoringu, které může zaměstnavatel zvolit. Hlavní principy monitoringu zůstávají i u těchto způsobů stejné.

Fotopasti

Podle metodiky ÚOOÚ spadají fotopasti pod zařízení provádějící monitoring obrazovým záznamem a jejich použití se tak bude řídit podle ustanovení § 316 odst. 2) ZP stejně, jako pořizování kamerových záznamů.

Čipy/karty

Využívání čipů či karet pro přístup na pracoviště je v dnešní době běžnou praxí. Zaznamenávání přístupů a odchodů zaměstnance do a ze zaměstnání nespadá pod monitoring ve smyslu ustanovení § 316 odst. 2) ZP.[34] V tomto případě je však nutné rozlišovat, zda dochází ke sběru osobních údajů zaměstnanců, především pak zda jsou vytvářeny záznamy o jejich příchodu a odchodu do zaměstnání, či nikoli. V případě, že dochází k pořizování záznamů, dochází tím ke sběru osobních údajů, je nutné o tom zaměstnance předem informovat. Zaměstnavatel je pak stejně jako v ostatních případech omezen účelem, za kterým je záznam příchodů a odchodů pořizován. Pokud by se zaměstnavatel rozhodl monitorovat zaměstnance skrze přístupové karty např. za účelem kontroly jejich polohy na pracovišti, musel by posoudit, zda tento zásah do soukromí zaměstnance není nepřiměřený, a zda neexistuje jiné dostatečné opatření pro dosažení vymezeného účelu, jako např. již dříve zmíněná kontrola vedoucím zaměstnancem.

[33] Prouza, J. Zpracování biometrických údajů zaměstnanců [online]. *epravo.cz.* [cit. 12. 9. 2024]. https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-zamestnancu-109845.html
[34] Nonnemann, F. Soukromí na pracovišti. *Právní rozhledy*. 2015, č. 7, s. 229.

Mystery shopping

Další specifickou formou monitoringu zaměstnance je tzv. mystery shopping, který spočívá v tom, že zaměstnavatel zkoumá, jakým způsobem zaměstnanec vystupuje vůči zaměstnancům, jaké jsou jeho prodejní schopnosti a jakým způsobem poskytuje služby zákazníkům. Tato kontrola probíhá na anonymní bázi, tak, aby bylo jednání zaměstnance zaznamenáno jako kdyby jednal se skutečným zákazníkem. Tato kontrola se může uskutečňovat i ve formě e-mailové komunikace, nebo telefonních hovorů. Mystery shopping stejně jako předešlá kategorie zpravidla nespadá pod ustanovení § 316 odst. 2) ZP hlavně z toho důvodu, že zaměstnanci jsou podrobení monitoringu pouze ohledně výkonu práce, tedy jednání se zákazníkem a jedná se o jednorázový záznam.[35]V případě, že jsou při mystery shoppingu pořizovány audiovizuální záznamy zaměstnanců, jedná se o zpracování osobních údajů a zaměstnavatel je stejně jako v předchozím případě povinen postupovat v souladu s GDPR.

[35] Nonnemann. Soukromí na pracovišti, s. 229.

8. KOMPARACE ČESKÉ PRÁVNÍ ÚPRAVY S VYBRANÝMI PRÁVNÍMI SYSTÉMY

Pro inspiraci pro přijetí rozhodnutí o vhodnosti případné legislativní změny v určité právní oblasti je vhodné seznámit se také se zahraniční úpravou dané problematiky. Pro účely tohoto souhrnu jsme se omezili pouze na tři, státy EU, které však jsou pro tento souhrn relevantní mj. pro rozdílnost jejich přístupu. Námi vybranými státy jsou Finsko, Francie a Německo.

8.1. Finsko

Finská právní úprava je při nastavení ochrany zaměstnanců před zasahováním do soukromí ze strany zaměstnavatele značně konkrétnější než úprava česká. O tom svědčí už existence samostatného zákona o ochraně soukromí v pracovním životě, který je speciální úpravou vůči zákonu o ochraně dat.

8.1.1. Obecná úprava

Finská ústava

Finská ústava[36] zakládá právo na soukromí v čl. 10, který zaručuje právo každého na osobní život, čest a nedotknutelnost domova s tím, že podrobnější úpravu vymezí zákon.

Čl. 12 stanoví, že vlastnické právo každé osoby požívá ochrany.

Zákon o ochraně dat

Zákon o ochraně dat[37] slouží jako obecný předpis o ochraně dat, který v kontextu zpracování dat na pracovišti odkazuje na speciální úpravu, tj. na zákon o ochraně soukromí v pracovním životě. V daném ustanovení konkrétně stojí: „*ustanovení o zpracování osobních dat zaměstnanců, provádění testů a zkoušek na zaměstnancích a související požadavky technické kontroly na pracovišti a opatřování a otevírání*

[36] Section 10 of the Constitution Act of Finland, 17 July 1919. Finsko.
[37] Section 30 of Data Protection Act 1052/2018. Finsko.

e-mailových zpráv zaměstnanců jsou zakotveny v zákoně o ochraně soukromí v pracovním životě."

Zákon o spolupráci

Finský zákon o spolupráci[38] ukládá zaměstnavateli povinnost konzultovat se zástupcem zaměstnanců, jakým způsobem by měly strany postupovat, aby docházelo k vývoji kultury na pracovišti tak, aby byly šetřeny práva a povinnosti obou stran a zároveň docházelo k pro obě strany příznivému vývoji. Články 8 a 12 konkrétně zavádí povinnost konzultací zaměstnavatele se zástupcem zaměstnanců v případech, kdy dochází ke sběru osobních údajů zaměstnanců. Zaměstnavatel tedy při zavádění monitoringu zaměstnanců musí nejprve dané opatření konzultovat se zástupcem zaměstnanců a informovat zaměstnance o rozhodnutích, týkajících se zaměstnanců, která hodlá přijmout. Zaměstnavatel by měl na žádost zaměstnanců podle čl. 24 vypracovat písemný záznam o prodiskutovaných záležitostech, který, pokud odpovídá jednání stran, podepíší obě jednající strany. Zaměstnavatel však není těmito konzultacemi vázán a může zavést monitoring i v případě, že je mu ze strany zástupce zaměstnanců doporučeno monitoring nezavádět. Cílem této úpravy je tedy otevření dialogu mezi zaměstnancem a zaměstnavatelem a alespoň částečné narovnání informační nerovnosti mezi zaměstnanci a zaměstnavatelem.

Zákon o ochraně soukromí v pracovním životě

V zákoně o ochraně soukromí v pracovním životě[39] jsou podrobně upravena pravidla monitoringu zaměstnanců na pracovišti. Bylo by neúčelné zabývat se tímto zákonem v celém jeho rozsahu, a proto níže zmíníme strukturu tohoto zákona a podrobněji rozebereme pouze vybraná ustanovení.

Tento zákon se dělí na 8 kapitol a celkem 26 ustanovení:

1. Obecná ustanovení
2. Obecné podmínky pro zpracovávání osobních údajů
3. Zpracovávání dat týkajících se užívání návykových látek

[38] Cooperation act 1333/2021. Finsko.
[39] Act on Protection of Privacy in Working life 759/2004. Finsko.

4. Podmínky týkající se podrobování zaměstnanců testům a zkouškám
5. Kamerový dohled na pracovišti
6. Opatřování a otevírání elektronických zpráv náležících zaměstnavateli
7. Ostatní ustanovení
8. Vstup v platnost

Nejrelevantnější pro monitoring zaměstnanců jsou ustanovení 16 až 20 obsažená v kapitolách 5 a 6.

V **sekci 16** je podrobně vymezeno, kdy je zaměstnavatel oprávněn zavést kamerový dohled na pracovišti. Mezi tyto účely patří zajištění osobní bezpečnosti zaměstnanců a dalších osob v prostorách, ochrana majetku, dohlížení na výrobní procesy, prevence nebo zkoumání situací ohrožující bezpečí, majetek nebo výrobní proces. Zároveň je dán zákaz pro použití kamerového dohledu v hygienických zařízeních a šatnách.

Mimo výše uvedené případy lze zaměřit kamerový dohled na stanoviště, na kterých zaměstnanci vykonávají práci, zejména kamerový dohled nezbytný pro prevenci zjevného nebezpečí násilí spojeného s prací zaměstnance nebo zjevnou škodu nebo nebezpečí vůči zaměstnancovu bezpečí nebo zdraví. Dále kamerový dohled nezbytný pro prevenci, nebo šetření majetkové trestné činnosti, pokud podstatná část zaměstnancovy práce spočívá v nakládání s majetkem vysoké hodnoty, jako jsou peníze, cenné papíry, nebo jiné cennosti. Dále je umožněn kamerový dohled k ochraně zaměstnancových zájmů a práv, kdy je kamerový dohled zřízen na základě žádosti zaměstnance, který je subjektem dohledu.

V **sekci 17** je upravena transparentnost kamerového dohledu, kdy zaměstnavatel při plánování a zavedení musí zvážit nebo zajistit dostupné alternativy, zda nebude zasaženo do soukromí zaměstnance více, než je třeba, aby nebyly záznamy využity pro jiné účely, aby byli zaměstnanci dostatečně informování, a aby byla umístěna označení v místech, na kterých k monitoringu dochází. Dále tato sekce stanoví, kdy mohou být záznamy použity mimo účel stanovený při zahájení monitoringu, a to především, pokud je záznam použit pro rozvázání pracovního poměru se zaměstnancem, pokud slouží k šetření diskriminace, sexuálního obtěžování, či jiného obtěžování mezi zaměstnanci nebo při šetření nebezpečí nebo vzniku pracovního úrazu. Poslední část sekce se věnuje době uchování, kdy je zaměstnavatel povinen záznam zničit, jakmile uplyne stanovená lhůta pro jeho uchování. V případě, že však záznam potřebuje

uchovat po delší dobu pro výše uvedené výjimky, nebo pokud existuje nějaký další závažný důvod, může tyto nahrávky uchovat do opadnutí tohoto důvodu.

Sekce 18 se zabývá opatřováním a otevíráním emailové komunikace zaměstnance a k tomuto jsou v ní dány základní předpoklady. Zaměstnavatel má právo opatřit a otevřít e-mailové zprávy zaslané na e-mailovou adresu, která byla zaměstnanci zaměstnavatelem svěřena, jestliže zaměstnavatel naplánoval a provedl nezbytná opatření k ochraně zaměstnancovy korespondence. Konkrétně se jedná o požadavek nastavení automatické odpovědi, informující o absenci zaměstnance, o její délce a o osobě odpovědné za přebírání zpráv adresovaných zaměstnanci, nebo požadavek na přesměrování pošty na jiného zaměstnance schváleného zaměstnavatelem, nebo požadavek na zvolení osoby, kterou odsouhlasí zaměstnavatel, která posoudí, jestli je e-mailová komunikace určena zaměstnavateli, nebo je soukromou korespondencí zaměstnance.

Sekce 19 se zabývá opatřováním komunikace zaměstnance v případě, že zaměstnavatel není správcem systému, na kterém byla daná komunikace vedena. Pro účely tohoto dokumentu však není důvodné se jimi podrobněji zabývat.

Sekce 20 se zabývá otevíráním korespondence opatřené podle sekce 19 a za zmínku stojí, že zaměstnavatel je o tomto otevření a opatření zprávy povinen vypracovat hlášení, které je bez zbytečného odkladu povinen předat zaměstnanci.

Úřad ombudsmana pro ochranu osobních údajů

Obdobou českého ÚOOÚ je finský Úřad ombudsmana pro ochranu osobních údajů, který je pověřen zkoumáním, zda jsou dodržována práva subjektů údajů, ukládáním pokut v souvislosti s osobními údaji a tvorbou vyjádření k problematice ochrany osobních údajů ve Finsku.

Tento úřad na svých webových stránkách obšírně zpracovává i problematiku monitoringu zaměstnanců, čímž dává zaměstnavatelům a zaměstnancům jasný přehled o tom, v jakých mezích může být monitoring prováděn.

8.1.2. Srovnání finské s českou úpravou

Jak je již z výše uvedeného patrno, hlavním rozdílem, mezi oběma úpravami je především jejich rozsah. Finsko ve svém Zákoně o ochraně soukromí v pracovním životě

nastavilo podstatně jasnější mantinely, ve kterých se musí finští zaměstnavatelé pohybovat v případě, že chtějí provádět monitoring zaměstnanců. To lze ilustrovat například na monitoringu prováděném pomocí kamerového systému. Finský zákonodárce tento způsob monitoringu upravuje v několika paragrafech, kdy každý z těchto paragrafů obsahuje několik odstavců, ve kterých jsou vymezeny určité podmínky a situace, za kterých je možné monitoring provádět. Mimo jiné tento zákon jasně a taxativně stanoví důvody, pro které je možné kamerové systémy na pracovišti instalovat, určuje prostory, ve kterých je monitorování kamerovým systémem zakázáno a vymezuje také prostory, které je možné nepřetržitě snímat pouze za určitých okolností, čímž je stálé pracovní stanoviště zaměstnance, kdy takovými výjimečnými okolnostmi jsou situace, kdy výkon práce zaměstnance je spojen s rizikem násilí a újmy na majetku, zdraví či životě (takovou pracovní pozicí může být například prodavač na benzinové pumpě, ostraha vchodu banky apod.). Oproti tomu český zákonodárce se zabývá monitoringem zaměstnanců skrze kamerové systémy v odst. 2) § 316 ZP, který čítá pouze jedno souvětí obsahující neurčitý právní pojem „zvláštní povaha činnosti zaměstnavatele".

Další rozdíl spočívá v činnosti národních úřadů pro ochranu osobních údajů, kdy ÚOOÚ sice vydává metodiky a stanoviska k určitým druhům monitoringu zaměstnanců, jedná se však spíše o činnost nahodilou a nejsou jí pokryty zdaleka všechny možné způsoby monitoringu zaměstnanců. Oproti tomu finský Úřad ombudsmana pro ochranu osobních údajů je v této oblasti poměrně aktivní, kdy ať už z jeho rozhodnutí, webových stránek nebo příručky ochrany osobních údajů v rámci pracovního života[40], mohou finští zaměstnavatelé snadněji určit, zda jimi zvolený postup spadá do zákonného rámce, či nikoli. Oproti tomu český zaměstnavatel, i v případě, že bude postupovat např. podle metodiky zavádění kamerových systému vypracované ÚOOÚ, nemá jistotu, že zavedení kamerového systému je v souladu se zákonem, což vede k tomu, že český zaměstnavatel vždy zavádí monitoring v nejistotě a hrozí mu sankce za to, že nevyhodnotil situaci správně.

Dalším rozdílem mezi úpravami je povinnost finského zaměstnavatele konzultovat zavedení monitoringu zaměstnanců se zástupcem zaměstnanců a o tomto jednání

[40] Office of the Data Protection Ombudsman. Handbook on Data Protection at Work [online]. *tietosuoja.fi.* [cit. 9. 6. 2024] https://tietosuoja.fi/documents/6927448/8214540/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+2020-+Tietosuojavaltuutetun+toimisto.pdf

na žádost zástupce vypracovat záznam. Povinnou konzultací je v podstatě zavedena povinnost zaměstnavatele zaměstnance o plánovaném monitoringu informovat, s výjimkou případů, kdy by informování o plánovaném monitoringu mohlo vést ke zmaření jeho účelu. Oproti tomu český zaměstnavatel má povinnost konzultovat zavedení monitoringu zaměstnanců s odborovou organizací pouze v případě, že se týká většího počtu zaměstnanců.

Z výše uvedeného pak lze vyvodit, že konkrétnost finské právní úpravy společně s činností Úřadu ombudsmana pro ochranu osobních údajů vytváří právní prostředí, ve kterém zaměstnavatel může chránit své zájmy v poměrně širokém rozsahu. Zároveň také díky svojí konkrétnosti dostatečně chrání zaměstnance před nepřiměřenými zásahy do soukromí. Finskou úpravu lze tedy považovat za zdařilou a vhodnou k tomu, aby byla alespoň z části použita jako inspirace při posuzování, jakým směrem by se měla ubírat úprava česká.

8.2. Francie

Francouzská úprava je oproti finské konstruována méně konkrétněji s tím, že právo na soukromí není obsaženo v Ústavě z roku 1958, a právo na soukromí občanů Francie tak vyplývá především z mezinárodních smluv a z podústavních předpisů, jako je francouzský zákon o ochraně osobních údajů, občanský zákoník a zákoník práce. Neexistuje však žádný specifický zákon, který by upravoval monitoring zaměstnanců v takové míře, jako je tomu ve Finsku a francouzská úprava tak zůstává velice stručná a nekonkrétní, což umožňuje větší prostor pro dotváření práva soudy a orgány státní správy.

Kromě vnitrostátních soudů, je nejvýznamnějším aktérem na poli monitoringu zaměstnanců ve Francii Francouzský úřad pro ochranu osobních údajů, zkracován jako CNIL, který obdobně jako ÚOOÚ vydává nezávazné pokyny při jejichž dodržování by měl zaměstnavatel postupovat v souladu se zákonem. Tyto pokyny však vydává ve značně větší míře, právě z důvodu stručnosti francouzské právní úpravy. Mezi tyto pokyny patří např. Pokyny k pořizování videozáznamů nebo snímků obrazovky ve spojení s nahráváním telefonických rozhovorů v práci, Pokyny ke kamerovému systému – kamerová ochrana na pracovišti, Zjednodušená norma č. 57 o odposlechu a záznamu hovorů na pracovišti.

8.2.1. Obecná úprava

Občanský zákoník

Francouzský občanský zákoník[41] ve svém čl. 9 stanovuje, že každý má právo na respektování jeho soukromého života. V tomto zákoně již žádné další zmínky o právu na soukromí nenalezneme.

Zákoník práce

Francouzský zákoník práce[42] stanoví v knize I, hlavě II. části L 1121-1, že nikdo nesmí omezovat práva jednotlivců nebo kolektivní svobody způsobem, který není odůvodněn povahou daného úkolu nebo cíle.

Podle knihy III, hlavy I, kapitoly II části L 2312-8 odst. 2) je zaměstnavatel povinen informovat sociální a ekonomický výbor, útvar reprezentující zaměstnance, o opatřeních zaváděných na pracovišti, o změnách pracovních podmínek a o zavádění nových technologií, nebo jakýchkoli významných změn pracovních podmínek.

Zákon č. 78-17 o zpracování údajů, souborech údajů a osobních svobodách

Francouzský zákon o zpracování údajů[43] stanovuje, že osobní údaje musí být zpracovány korektně, zákonně a transparentně s ohledem na subjekt údajů. Dále musí být osobní údaje získány pro konkrétní, výslovně vyjádřené a legitimní účely, v rozporu s nimiž nesmí být zpracovány, musí být přesné a v případě potřeby aktualizované, zabezpečené a pokud není dán zvláštní důvod, nesmí být uchovávány déle, než pět let.

Zároveň v čl. 48 odkazuje na čl. 13 GDPR, který zavádí povinnost zpracovatele osobních údajů informovat subjekt osobních údajů o jejich zpracování.

[41] Article 9 de la loi n° 70-643, Code civil. Francie.
[42] Code du travail. Francie.
[43] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Francie.

8.2.2. Vybraná rozhodnutí

Rozhodnutí č. 99-42942 ze dne 1. 10. 2001

Nikon France vs. Onof

V tomto rozhodnutí francouzský Kasační soud[44] poprvé rozhodl, že zaměstnanci mají právo na soukromí také na pracovišti zaměstnavatele. Také rozhodl, že se zaměstnavatel dopustil porušení práva na soukromí zaměstnance, když prohledal jeho pracovní počítač. Toto rozhodnutí však bylo již prolomeno a momentálně francouzská rozhodovací praxe zastává ten názor, že pokud nebyly soubory na pracovním počítači zaměstnavatele jasně označeny jako soukromé, může je zaměstnavatel otevřít a případně na jejich základě vyvodit důsledky pro zaměstnance.

Rozhodnutí č.°San-2023-021 ze dne 27. 12. 2023

Amazon

Francouzský úřad pro ochranu osobních údajů rozhodl dne 27. 12. 2023 o uložení pokuty ve výši 32 mil. euro společnosti AMAZON FRANCE LOGISTIQUE, spravující největší logistický sklad skupiny Amazon ve Francii, která se dopustila několika porušení GDPR. Ta spočívala především v tom, že společnost nepostupovala v souladu s principem minimalizace podle čl. 5 odst. 1) GDPR, když sbírala a zpracovávala data o výkonnosti zaměstnanců v nepřiměřeném rozsahu, a uchovávala je po nepřiměřeně dlouhou dobu.[45]

8.2.3. Vybrané pokyny CNIL

Dohled prostřednictvím kamerových záznamů při práci[46]

V rámci pokynu o dohledu prostřednictvím kamerových záznamů se CNIL věnuje především tomu, jaká opatření či povinnosti je třeba dodržovat při instalaci kamer. Mezi tyto povinnosti patří zákaz natáčení zaměstnance na jeho pracovišti, s výjimkou zvláštních okolností (manipulace s penězi či sklad s cenným zbožím), zákaz natáčení prostorů sloužících k přestávce, odpočinku či hygieně zaměstnanců nebo také zákaz

[44] Rozhodnutí francouzského Kasačního soudu ze dne 1. 10. 2001, č. 99-42942.
[45] Rozhodnutí francouzského úřadu pro ochranu osobních údajů ze dne 27. 12. 2023, č. °San-2023-021.
[46] Commission nationale de l'informatique et des libertés. La vidéosurveillance – vidéoprotection au travail [online]. *cnil.fr.* [25. 4. 2024]. https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail

natáčení prostor odborových organizací a dalších zástupců zaměstnanců. Součástí pokynu jsou také informace o tom, kdo si může prohlížet záznamy z kamer, jak dlouho je možné záznamy uchovávat, jakým způsobem je třeba zaměstnance informovat o kamerovém dohledu či jaké další formální povinnosti je třeba splnit. Pokyn představuje přehledný návod pro zaměstnavatele, jehož obsahem je i grafické znázornění přípustného použití kamer či značek informujících o kamerovém dohledu.

Biometrická kontrola přístupu na pracovišti[47]

Vzhledem ke stále rostoucí popularitě používání biometrické kontroly publikoval CNIL pokyny i k této oblasti, a to konkrétně k biometrické kontrole přístupu do prostor, počítačů nebo aplikací na pracovišti. Součástí pokynu je vysvětlení regulačního rámce biometrické kontroly, a zároveň jednoduchý návod sestavený z několika kroků pro postup zaměstnavatelů v případě, že by na svých pracovištích chtěli takovou kontrolu zavést. V souvislosti s tímto pokynem vydal CNIL také závazné vzorové nařízení o biometrii na pracovišti,[48] které specifikuje a upřesňuje povinnosti zaměstnavatelů, kteří biometrická zařízení chtějí používat.

Geolokace vozidel zaměstnanců[49]

Nejnovějším ze zmíněných pokynů CNIL je pokyn týkající se geolokace vozidel zaměstnanců. V rámci pokynu je stručně uvedeno, pro jaké účely je možné geolokaci využít, a to např. pro účely zajištění bezpečnosti zaměstnance, zboží nebo vozidel, která mají na starosti, a zejména pro účel nalezení vozidla v případě krádeže, nebo také sledování pracovní doby, pokud to nelze provést jiným způsobem. Geolokaci nicméně nelze použít pro účel kontroly dodržování rychlostních limitů, neustálé kontroly zaměstnance nebo pro výpočet pracovní doby zaměstnance, jestliže pro kontrolu

[47] Commission nationale de l'informatique et des libertés. Le contrôle d'accès biométrique sur les lieux de travail [online]. *cnil.fr.* [25. 4. 2024]. https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail

[48] Commission nationale de l'informatique et des libertés. Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail [online]. *cnil.fr.* [25. 4. 2024]. https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf

[49] Commission nationale de l'informatique et des libertés. La géolocalisation des véhicules des salariés [online]. *cnil.fr.* [25. 4. 2024]. https://www.cnil.fr/fr/la-geolocalisation-des-vehicules-des-salaries

již existuje jiný systém. V rámci pokynu se CNIL vyjadřuje také k právům kontrolovaných zaměstnanců, přístupu k informacím z geolokačního zařízení či k délce jejich uchovávaní.

8.2.4. Srovnání s českou úpravou

Francouzská právní úprava, stejně jako česká právní úprava, neupravuje monitoring zaměstnanců v samostatném předpise, avšak na rozdíl od české právní úpravy neobsahuje žádné ustanovení, které by upravovalo monitoring zaměstnanců výslovně. Z výše uvedeného vyplývá, že česká právní úprava, i přes její stručnost, je oproti té francouzské o něco konkrétnější. Českému zaměstnavateli je v zákoně sděleno alespoň obecně, kdy je oprávněn zaměstnance monitorovat, jakým způsobem a zda je povinen o monitoringu zaměstnance informovat. Absence úpravy ve francouzské legislativě sice dává větší prostor zaměstnavatelům pro zavádění monitoringu zaměstnanců, to je však podmíněno tím, že zaměstnavatel musí provést posouzení přiměřenosti zaváděného opatření, k čemuž mu slouží pouze nařízení GDPR, stanoviska CNIL a předchozí soudní rozhodnutí. Absence konkrétní právní úpravy se tak nerovná vyšší míře oprávnění zaměstnavatele zavádět monitoring zaměstnanců, neboť bez vymezených hranic je posouzení, zda zaměstnavatel postupoval v souladu či rozporu se zákonem, čistě na uvážení soudů a orgánů státní správy. Je však potřeba zdůraznit, že stanoviska CNIL platí v Evropské unii za velmi kvalitní a jsou mnohdy používána jako vzory pro výklad norem na ochranu osobních údajů.

Mezi konkrétnější rozdíly pak patří především povinnost francouzského zaměstnavatele informovat sociální a ekonomický výbor ohledně zavádění monitoringu zaměstnanců, a povinnost informovat zaměstnance o zpracovávání jeho osobních údajů.

8.3. Německo

Monitoring zaměstnanců v Německu, stejně jako ve Francii není výslovně upraven v žádném zákoně, nebo jeho ustanovení. Opírá se tedy především o úpravu v GDPR s tím, že v některých případech zákony rozšiřují situace, ve kterých lze osobní údaje zpracovávat.

8.3.1. Obecná úprava

Základní zákon Spolkové republiky Německo

Německý základní zákon[50] výslovně nestanoví ani právo jednotlivce na soukromí, ani se nezabývá monitoringem zaměstnanců. Jediným pro monitoring relevantním ustanovením je čl.10 ve kterém je zakotveno právo na zachování listovního tajemství vztahující se na korespondenci, poštu a telekomunikaci.

Spolkový zákon o ochraně osobních údajů

Spolkový zákon o ochraně osobních údajů[51] v §26 upravuje zpracování osobních údajů pro účely pracovního poměru. Tento paragraf je dále rozdělen do osmi odstavců s tím, že pravidla pro monitoring zaměstnanců nejvíce upravují odstavce 1), 3) a 4). **Odst. 1)** stanoví, že osobní údaje zaměstnance mohou být zpracovány za účelem odhalení trestné činnosti pouze v případě, že lze na základě zaznamenáno podezření předpokládat, že subjekt údajů spáchal trestný čin při zaměstnání a zpracování takových dat je nutné pro vyšetření trestné činnosti a zároveň v dané situaci nepřevažuje oprávněný zájem subjektu osobních údajů.

Odst. 3) umožňuje zaměstnavateli zpracovávat osobní údaje patřící podle GDPR do zvláštní kategorie pro účely spojené se zaměstnáváním v případě, že je jejich zpracování nutné pro uplatnění práv, nebo plnění povinností plynoucích ze zákona, zejména z oblastí pracovního práva, sociálního zabezpečení v případech, kdy zaměstnavatel nepředpokládá, že existuje oprávněný důvod zaměstnance, který by zpracování těchto údajů vylučoval.

Odst. 4) stanoví, že zpracování osobních údajů zaměstnanců pro účely spojené se zaměstnáváním může být povoleno na základě kolektivní smlouvy.

Zákon o organizaci pracovních vztahů v podniku

V tomto zákoně jsou upraveny podnikové rady a jejich pozice vůči zaměstnancům a zaměstnavateli. Důležitým ustanovením je pak ustanovení **§ 87 odst. 1) bodu 6)**,

[50] Law number 100-1, Basic Law for the Federal Republic of Germany. Německo.
[51] Section 26 of Federal data protection act. Německo.

které říká, že podniková rada má právo spolurozhodovat o záležitostech týkajících se zavedení a užívání technických prostředků určených pro monitorování chování nebo pracovní výkonnosti zaměstnanců.

Telekomunikační zákon a telemediální zákon

Telekomunikační zákon a telemediální zákon upravují postavení poskytovatelů telekomunikačních a telemediálních služeb. Zaměstnavatel v obecné rovině není poskytovatelem těchto služeb, z pohledu německých úřadů se jím však může stát v případě, že zaměstnavatel poskytne zaměstnanci zařízení telekomunikačních, nebo telemediálních systémů pro osobní potřebu.[52] Tyto zákony pak zakazují poskytovateli služeb monitorovat komunikaci uživatelů a zpracovávat informace o přístupu uživatelů na webové stránky.

Úřady pro ochranu údajů

Německo, na rozdíl od ostatních výše zmíněných států, má více úřadů pro ochranu údajů, s tím, že každá spolková republika má jeden takový úřad. Vedle těch existuje také Úřad spolkového komisaře pro ochranu dat a svobodu informací. Ty společně vydávají tzv. „krátké listy“ ve kterých se zabývají právy na ochranu osobních údajů zaměstnanců. Činnost úřadů pro ochranu údajů v Německu je v rámci publikací metodik a výkladů zákonů právního nastavení monitoringu zaměstnanců výrazně nižší než v ostatních státech s tím, že hlavními východisky při posuzování zákonnosti postupů zaměstnavatelů při monitoringu zaměstnanců jsou rozhodnutí soudů a jednotlivých úřadů.

[52] Bach, S. and Holger, L. Employee Monitoring (Germany) [online]. *bakermckenzie.com.* [cit. 13. 9. 2024]. https://www.bakermckenzie.com/-/media/files/people/bach-simone/ar_germany_employeemonitoring_2019.pdf?la=en

8.3.2. Vybraná rozhodnutí

Rozhodnutí Federálního pracovního soudu sp. zn. 1 ABR 34/03 ze dne 14. 12. 2004
Deutsche Post AG.

Německý Federální pracovní soud[53] v tomto rozhodnutí shledal nepřiměřeným zásahem videomonitoring zaměstnanců nakládajících se zásilkami. Cílem videomonitoringu zaměstnavatele bylo snížit množství kradených a otevíraných zásilek, přičemž doba, po kterou byli zaměstnanci monitorováni nebyla předem přesně stanovena, vždy se však mělo jednat o minimálně 20, maximálně 60 hodin týdně. Soud považoval zejména za problematické, že zaměstnanec neměl možnost vědět, zda je na pracovišti sledován po celou pracovní dobu či nikoli, a tak musel počítat s tím, že je sledována neustále.

Rozhodnutí Federálního pracovního soudu sp.zn. 2 AZR 681/16 ze dne 27. 7. 2017

Soud v rámci soudního řízení shledal nezákonným důkaz získaný zaměstnavatelem na základě použití keyloggeru, o kterém sice byl zaměstnanec informován, avšak bylo mu zamlčeno, že monitorování bude probíhat trvale na celém zařízení nejen při využívání internetového připojení. Použití takovéhoto důkazu bylo dle Federálního pracovního soudu neslučitelné s právem zaměstnance na informační sebeurčení, jelikož zaměstnanec o monitoringu nevěděl, monitoring byl trvalý a nebyl odůvodněn jakýmkoliv podezřením zaměstnavatele na trestnou činnost nebo jiné závažné porušení povinností.

8.3.3. Vybrané krátké listy

Krátký list č. 14 – ochrana údajů zaměstnanců[54]

Tento dokument slouží jako prvotní návod pro neveřejný sektor, jak by se mělo GDPR uplatňovat v praxi. Dokument především odkazuje na čl. 88 odst. 1 GDPR týkající se zpracování údajů v souvislosti se zaměstnáním. Na základě tohoto článku byl dle dokumentu přijat § 26 spolkového zákona o ochraně osobních údajů,

[53] Rozhodnutí německého Federálního pracovního soudu ze dne 14. 12. 2008, sp. zn. 1 ABR 34/03.
[54] Datenschutzkonferenz. Kurzpapier Nummer 14 Beschäftigtendatenschutz [online]. *datenschutzkonferenz-online.de.* [23. 5. 2024]. https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf

kterému se zbytek dokumentu věnuje. Dokument tak uvádí podrobnější informace o obsahu § 26 zákona, a to konkrétně ke zpracování údajů pro účely pracovního poměru, zpracování údajů pro odhalování trestných činů, zpracování zvláštních kategorií osobních údajů a zpracování údajů mimo datové systémy. Součástí dokumentu je také stručná informace o právních důsledcích porušení povinností podle § 26.

Krátký list č. 15 – videodohled[55]

Stejně jako předchozí krátký list, byl tento dokument vypracován za účelem poskytnutí stručných informací o tom, jak by se mělo GDPR uplatňovat v praxi, ovšem ve vztahu ke kamerovému dohledu. Dokument se prvně věnuje relevantním ustanovením GDPR pro kamerový dohled a požadavkům na něj, jako je zákonnost či transparentnost. Součástí dokumentu jsou také informace o době skladování údajů z kamerového systému, způsobu provedení pořizování, instalace a provozování kamerových systémů a informace dalších formálních požadavcích na kamerové systémy.

8.3.4. Srovnání s českou úpravou

Z výše popsaného opět plyne, že Německá úprava je vůči České úpravě méně konkrétní a monitoring zaměstnanců se řídí především podle nařízení GDPR a praxe nastavené v rozhodnutích soudů a úřadů na ochranu osobních údajů. Větší množství úřadů na ochranu osobních údajů může vést ke zkvalitnění a větší četnosti stanovisek jednotlivých úřadů.

8.4. Zhodnocení a srovnání právních úprav

Z výše uvedeného vyplývá, že nejpropracovanější legislativní systém monitoringu zaměstnanců má nastaveno Finsko, které lze považovat za velmi pokrokovou zemi i z pohledu digitalizace a používání informačních technologií. Pro zaměstnavatele se finská právní úprava zdá být přehledná a poměrně jasně stanovuje podmínky, pro zavedení monitoringu. Konkrétnější právní úprava, kterou zde vidíme, však může být problematická s ohledem na rychlý vývoj v technologickém prostředí a s tím související

[55] Datenschutzkonferenz. Kurzpapier Nr. 15 Videoüberwachung nach der Datenschutz-Grundverordnung [online]. *datenschutzkonferenz-online.de.* [23. 5. 2024]. https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf

nutnost novelizací právních předpisů. Rovněž je zde dán menší prostor pro soudy, aby právo dotvářely. Celkově je však nutné finskou právní úpravu hodnotit jako kvalitní. K vysokému standardu této právní úpravy dopomáhá i činnost Úřadu ombudsmana pro ochranu osobních údajů.

Naproti tomu je francouzská právní úprava spíše strohá. Při posouzení právního prostředí monitoringu zaměstnanců ve Francii je však potřeba vyzdvihnout činnost francouzského úřadu pro ochranu osobních údajů (CNIL), který je ve své činnosti velmi aktivní a přichází s řadou stanovisek, která mají dopad na ochranu osobních údajů v celé Evropské unii. Ve francouzské právní úpravě také můžeme sledovat tradičně silné propojení na zástupce zaměstnanců.

Právní úpravu monitoringu zaměstnanců v Německu je zaměřena primárně na ochranu osobních údajů zaměstnanců. Německý zákon na ochranu osobních údajů, na rozdíl od jeho české obdoby, přímo řeší i dopad na pracovněprávní vztahy. Jedná se tak o doplnění GDPR, nikoliv o stanovení mantinelů pro provádění monitoringu zaměstnanců. Oblast monitoringu zaměstnanců v širším slova smyslu je tvořena především soudními rozhodnutími. Jednotlivé spolkové úřady na ochranu osobních údajů dotvářejí právní rámec, přestože jejich stanoviska mají i zde pouze nezávazný charakter. Obdobně jako v případě Francie, zejména spolkový úřad v Bavorsku vytváří řadu kvalitních podkladů dopadajících na oblast ochrany soukromí a osobních údajů.

9. ÚVAHY DE LEGE FERENDA A MOŽNOST ROZVOLNĚNÍ

Jak vyplývá z provedené komparace právních úprav, česká právní úprava se nachází mezi kodifikovanou finskou právní úpravou a volnější právní úpravou zvolenou ve Francii.

Aby česká právní úprava lépe vyhovovala podmínkám moderní praxe, je potřeba koncept dotčených právních norem upravit či rozvolnit. Ustanovení § 316 ZP je z pohledu uživatelů velmi nepřehledné a výkladové problémy způsobuje i u odborné veřejnosti. Úplné odstranění ustanovení § 316 ZP způsobující absenci výslovné úpravy monitoringu v zákoně a pouhé opírání se o úpravu v GDPR, jak tomu je ve Francii či Německu, nepovažujeme za vhodné. Naopak máme za to, že § 316 ZP by měl doznat úprav.

Případná novelizace ustanovení § 316 ZP by zejména měla odstranit nejasnou úpravu obsaženou ve druhém odstavci, neboť právě ta způsobuje v praxi největší problémy. Právní úprava by měla opustit zcela zavádějící hypotézu zakazující monitoring „bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele“. Při srovnání zejména s finskou právní úpravou se nabízí právní úpravu monitoringu v České republice upravit lépe a přesněji, aby nedocházelo k interpretačním problémům. Stranám pracovněprávní vztahu by se dostalo větší jistoty ohledně toho, co ještě je či není dovoleno, čímž by se dosáhlo lepší ochrany jejich subjektivních práv.

Současně ale nepovažujeme za účelné, aby se právní úprava vztahovala pouze k vysloveně uvedených typům monitoringu, tak jak je tomu např. ve výše popsané finské právní úpravě. Taková právní úprava může být do budoucna příliš svazující. Právní úprava by se, na rozdíl od dnešního stavu, neměla limitovat pouze na otevřené nebo skryté sledování, odposlechy a záznamy telefonických hovorů, kontrolu elektronické pošty a kontrolu listovních zásilek adresovaných zaměstnanci, ale měla by se obecně vztahovat na všechny možné formy monitoringu. Tímto způsobem je možné docílit stálosti právní úpravy s ohledem na dynamicky se rozvíjející svět informačních technologií.

Dále by první úprava neměla zbytečně limitovat zaměstnavatele v zavedení monitoringu, pokud zvolený způsob monitoringu dokáže technologickými opatřeními poskytnout dostatečnou ochranu subjektům monitoringu jakož i jejich osobním údajům.

V návaznosti na novelizaci § 316 odst. 2 ZP musí dojít rovněž k úpravě § 316 odst. 3, který přímo navazuje na § 316 odst. 2 ZP. Pro naplnění požadavků praxe by měl zákonodárce určit, jak by měli zaměstnavatelé plnit informační povinnost a vzít v potaz,

že v některých situacích by konkrétní informování zaměstnance před provedením monitoringu mohlo zmařit zaměstnavatelem zamýšlený účel. Za vhodné považujeme zavést obecnou informační povinnost a postavit na jisto, že v případě potřeby akutního jednorázového zásahu do soukromí zaměstnance, je možné o tomto zásahu zaměstnance informovat až následně (to vše samozřejmě v neexcesivní podobě, ideálně při splnění testu proporcionality či přímo provedení balančního testu).

Nabízí se také možnost po vzoru finské právní úpravy zavést povinnost konzultací (projednání) zaměstnavatele se zástupcem zaměstnanců ve všech případech, kdy dochází k monitoringu zaměstnanců, tedy nejen v případech monitoringu většího počtu zaměstnanců. Zaměstnavatel by při zavádění monitoringu zaměstnanců musel nejprve dané opatření projednat s odborovou organizací a informovat zaměstnance o rozhodnutích, která hodlá přijmout. V úvahu připadá také při zavádění monitoringu vyžadovat namísto pouhého projednání souhlas odborové organizace. Povinnost zaměstnavatele získat souhlas je ale z našeho pohledu příliš restriktivní a zaměstnavatele by nepřiměřeně omezovala. Obdobnou úpravu, tj. angažování zástupců zaměstnanců (podnikové rady), obsahuje i německá právní úprava. Máme za to, že projednání zavedení monitoringu zaměstnanců s odborovou organizací či zástupci zaměstnanců, může výrazně zvýšit ochranu zaměstnanců. Na rozdíl od požadavku na souhlas odborové organizace nemusí být projednání této oblasti výraznou překážkou ani pro zaměstnavatele. Rovněž zakomponování projednání zavedení monitoringu do ZP může být vzhledem k systematice ZP poměrně snadné.

Přijetí zcela nového zákona pro oblast monitoringu zaměstnanců nepovažujeme za vhodné, neboť máme za to, že právní úprava by měla zůstat spíše minimalistická (jak je tomu ostatně i nyní), zároveň by měla být srozumitelná, což se v tuto chvíli bohužel neděje. Dle našeho názoru postačí novelizace menšího rozsahu, jak je na značeno výše.

Zároveň bychom považovali za přínosné, kdyby došlo ke zvýšení aktivity ÚOOÚ, který sice primárně neřeší monitoring zaměstnanců, jeho stanoviska se však týkají i monitorování zaměstnanců a jsou v praxi vítaným vodítkem. Vzorem pro budoucí činnost ÚOOÚ v oblasti vydávání stanovisek, doporučení či metodik by mohl být francouzský CNIL, jehož stanoviska či pokyny, jako např. výše zmíněné pokyny k biometrické kontrole přístupu na pracovišti, představují vhodný nástroj pro výklad právních norem. Zároveň jejich praktická využitelnost poskytuje zaměstnavatelům návod, jak postupovat při

zavádění různých systému kontroly na pracovišti. Některé dokumenty předkládané CNIL jsou psány praktickým jazykem, aby bylo možné je pochopit i bez dalšího právního vzdělání.

Za úvahu stojí také vydávání různých příruček po vzoru „krátkých listů“ německých úřadů pro ochranu osobních údajů, které by dávaly zaměstnavatelům shrnutí základních informací v oblasti ochrany osobních údajů a stručné instrukce pro zavádění monitoringu a uplatňování GDPR v praxi. Tento typ nezávazných dokumentů by tak mohl vhodně doplnit činnost ÚOOÚ a pomoct zaměstnavatelům při zavádění monitoringu. Opět forma krátkého a stručného dokumentu může být pro řadu zaměstnavatelů uživatelsky žádaná.

V oblasti ochrany osobních údajů zaměstnanců lze podle našeho názoru označit současnou právní úpravu (tj. zejména GDPR) za dostatečnou.

10. ZÁVĚR

V rámci analýzy bylo konstatováno, že česká právní úprava monitoringu zaměstnanců je pro praxi obtížně použitelná a rovněž množství judikatury není natolik široké, aby tyto obtíže pomohlo odstranit. Rovněž ÚOOÚ se problematikou monitoringu zaměstnanců zabývá spíše okrajově a neexistují tedy ani stanoviska, která by výkladové problémy dokázala překlenout.

Komparací zahraničních právních úprav bylo zjištěno, že vybrané státy Evropské unie používají různé přístupy k monitoringu zaměstnanců, ať již přijetím komplexní právní úpravy dané oblasti nebo spoléháním se pouze na judikaturu a výkladová stanoviska dohledových orgánů. Obecně se zdá, že činnost dozorových orgánů v zemích, jejichž právní úpravy byly porovnávány, je četnější a praktičtější, než je tomu v případ ÚOOÚ.

Dle našeho názoru by v České republice měl být monitoring zaměstnanců lépe legislativně zpracován, přičemž považujeme za vhodné novelizovat současnou právní úpravu (zejména ZP), před přijetím zcela nového zákona. Novelizace současného znění ZP by nemusela být extenzivní, naopak by postačily minimalistické úpravy, které by jen měly obecnou limitaci monitoringu zpřehlednit a zmodernizovat. V oblasti ochrany osobních údajů je zcela dostačující úprava na úrovni GDPR, které danou oblast řeší komplexně.

I nadále však musí zůstat zachován princip, že nesmí docházet k extenzivním zásahům do práva na soukromí zaměstnanců, a v jednotlivých případech zároveň musí být nutné posuzovat, zda zájem zaměstnavatele a jeho právo na ochranu majetku převáží zájem na ochraně soukromí zaměstnanců.