25. 6. 2019

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Monitoring činností zaměstnanců ze strany zaměstnavatele (1. část)

Aktivity zaměstnanců na pracovišti může zaměstnavatel monitorovat s využitím široké škály moderních technologií. Důvodem takového monitorování bývá například ochrana majetku zaměstnavatele (kontrola pomocí kamerového systému), kontrola výkonnosti zaměstnance (sledování aktivit zaměstnanců na internetu) či ochrana života a zdraví zaměstnavatele a zaměstnance (systém GPS). V souvislosti s tím vyvstává otázka, kdy a které z těchto nástrojů monitoringu může zaměstnavatel používat tak, aby nezákonně nezasahoval do garantovaného práva na ochranu soukromí.

Cílem tohoto článku, rozděleného do dvou částí, je poskytnout pohled na vybrané druhy monitoringu, vymezit jeho legální hranice a zhodnotit sankce hrozící zaměstnavateli.

Zákoník práce[1] v ustanovení § 316 odst. 1 stanovuje, že zaměstnanec nesmí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. V rámci realizace ochrany je dodržování tohoto zákazu zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.

Přiměřenost této kontroly spočívá především v tom, jak uvádí také § 316 zákoníku práce ve svém odst. 2 (a dále odst. 3), že zaměstnavatel nesmí bez závažného důvodu narušovat soukromí zaměstnance, a to tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.

Vedle zásady přiměřenosti vyplývá z obecné právní úpravy celá řada konkrétních povinností či zásad, které by zaměstnavatel při monitoringu svých zaměstnanců měl dodržovat. Jsou jimi zejména zásada proporcionality, zásada legitimity a zásada legality, které společně proklamují, že monitoring zaměstnanců nemá bezdůvodně zasahovat do práva na jejich soukromí a že zaměstnavatel musí mít pro zavádění jakéhokoliv monitoringu vážný důvod spočívající ve zvláštní povaze jeho činnosti. Naopak nejdůležitější povinností zaměstnavatele zůstává povinnost zaměstnance o monitoringu předem a náležitým způsobem informovat.

Zaměstnavatel se při používání těchto monitorovacích zařízení často stává také správcem osobních údajů zaměstnanců (např. při ukládání nahrávek z kamerového systému), a je proto dále třeba výše uvedenou úpravu zákoníku práce balancovat s regulací obsaženou v široce diskutované unijní úpravě ochrany osobních údajů, kterou představuje obecné nařízení o ochraně osobních údajů (GDPR)[2]. Základní východiska a limitace pro zpracování osobních údajů zaměstnanců představuje čl. 6 odst. 1 GDPR týkající se zákonnosti zpracování a čl. 13 a 14 GDPR upravující informační povinnost zaměstnavatele vůči zaměstnancům. Povinnosti z obou právních úprav jsou vedle sebe postaveny

paralelně.

Monitoring elektronické komunikace

Rozsahem monitoringu e-mailové komunikace se zabýval Úřad pro ochranu osobních údajů (dále také "**ÚOOÚ**"), který ve svém stanovisku č. 2/2009[3] uvedl rozdíl mezi použitím soukromé a pracovní e-mailové adresy a mezi soukromou a pracovní e-mailovou zprávou. E-mailová adresa zaměstnance, která je vedena na takzvaném free-mailovém serveru (například seznam.cz, gmail.com), je vždy považována za soukromou. Takovou e-mailovou adresu může zaměstnavatel otevřít a přečíst pouze výjimečně, v zájmu ochrany svých práv, a jestliže je z údajů uvedených v hlavičce zřejmé, že se jedná o pracovní email.

V případě, kdy e-mailová adresa patří zaměstnavateli, a je složena ze jména a příjmení zaměstnance, např. jan.svoboda@doména.cz jsou e-maily na ní doručené považovány také za soukromou elektronickou poštu. Takové emaily lze považovat za osobní údaj, avšak takový osobní údaj, k jehož zpracování a zveřejňování je zaměstnavatel oprávněn. Oproti tomu věcně konstruovaná e-mailová adresa, např. info@doména.cz, je i v případě, kdy je obhospodařována pouze jedním zaměstnancem považována za úřední (pracovní) elektronickou adresu. Při spravování takové adresy mohou být očekávání soukromí ze strany zaměstnanců minimální.[4]

Z judikatury ESLP lze zmínit rozhodnutí ve věci *Bărbulescu proti Rumunsku* (stížnost č. 61496/08). V posuzované věci si rumunský zaměstnanec pan Barbulescu zřídil na popud zaměstnavatele soukromý účet na síti Yahoo, na němž měl vyřizovat objednávky zákazníků. Tento účet poté využíval i pro další osobní komunikaci, a to i přesto, že mu zaměstnavatel takové užití zakázal. ESLP nejprve v lednu 2016 dospěl k závěru, že monitoring komunikace konkrétního zaměstnance během pracovní doby na počítači, který používá k plnění pracovních povinností, není v rozporu s čl. 8 Úmluvy o ochraně lidských práv a základních svobod. Poté však v září 2017 rozhodnutím Velkého senátu svůj verdikt změnil s odůvodněním, že pouhá informovanost zaměstnance o zákazu používání účtu elektronické komunikace pro soukromé účely není dostatečná.

Zdůraznil tak, že pokud společnosti chtějí sledovat komunikaci (analogicky budou tyto závěry použitelné i pro další způsoby monitoringu) svých zaměstnanců, nestačí pouhý zákaz používání pracovních pomůcek, ale musí tyto zaměstnance předem informovat také o možnosti a rozsahu plánovaných kontrol dodržování tohoto zákazu. Zaměstnavatelé rovněž potřebují legitimní důvod k provedení kontroly a musí v každém jednotlivém případě zvážit existenci mírnějších kontrolních opatření.

Domníváme se, že i s ohledem na výše uvedené je zákonné provádět tzv. anonymní monitorování e-mailů, tedy takové monitorování, které neumožňuje vyvodit závěry o konkrétních zaměstnancích a neumožňuje tyto jednotlivce identifikovat. K tomuto účelu mohou přiměřeně sloužit také nástroje Data Loss Prevention (DLP)[5], které automaticky monitorují např. odchozí e-maily za účelem zabránění neoprávněného přenosu chráněných údajů (např. osobních údajů klienta). Méně invazivní řešení bude také představovat např. namátková kontrola hlaviček e-mailů.

Odlišnou situaci představuje tzv. osobní monitoring, tedy cílené, adresné monitorování e-mailové komunikace konkrétního zaměstnance, které by, vzhledem k intenzitě zásahu do soukromí zaměstnance, neměl zaměstnavatel provádět bez závažného důvodu. Zároveň má zaměstnavatel povinnost zaměstnance o možnosti provedení takového monitoringu předem informovat. Konkrétně takovou kontrolu lze provést pouze v případě, že během běžné anonymní prohlídky (např. právě při kontrole hlaviček e-mailů) budou zjištěny nesrovnalosti a existuje důvodné podezření, že zaměstnanec např. prozrazuje obchodní tajemství či páchá trestný čin. Kontrolu e-mailů lze provést také v případě, že slouží k ochraně zaměstnanců při odhalování šikany či sexuálního obtěžování.

Sledování aktivity zaměstnanců na internetu

Analogické závěry lze vztáhnout i na sledování aktivit zaměstnanců na internetu. K této otázce se blíže vyjádřila i česká judikatura, kdy již v roce 2012 Nejvyšší soud vydal rozhodnutí známé pod názvem *Kasalova pila*[6], které posléze potvrdil i Ústavní soud, a ve kterém akceptoval kontrolu pohybu zaměstnance na internetu za účelem zjištění, zda zaměstnanec respektuje (a pokud nerespektuje, tak v jaké míře) zákaz používat výpočetní techniku zaměstnavatele pro svojí osobní potřebu. Toto své tvrzení poté o rok později Nejvyšší soud zopakoval, když v rozsudku ze dne 7. srpna 2014, sp. zn. 21 Cdo 747/2013 judikoval, že v případě, kdy cílem kontroly není zjišťování obsahu prohlížených stránek, ale jen to, zda zaměstnanec respektuje stanovený zákaz zaměstnavatele o používání počítače pro soukromé účely, jde o kontrolu přiměřenou a přípustnou.

Česká judikatura se tak odlišně od rozhodnutí ESLP ve věci *Bărbulescu* přiklonila na stranu zaměstnavatele. Obdobný postoj zaujímá i Nejvyšší soud Slovenské republiky, který ve svém rozsudku ze 12. září 2016, sp. zn. 3 Cdo 233/2015 uvedl, že pokud zaměstnavatel ve vnitřním předpise zakázal zaměstnancům používání přidělené výpočetní techniky pro soukromé účely, musí mít možnost kontroly tohoto zákazu.

Dále lze zmínit rozhodnutí Federálního pracovního soudu v Německu, který ve svém rozsudku ze dne 27. července 2017, sp. zn. 2 AZR 681/16, potvrdil zákaz monitorování činnosti zaměstnance (e-mailové adresy) pomocí tzv. keyloggeru.[7] V tomto rozsudku soud judikoval, že samotné monitorování počítače zaměstnanců lze (při dodržení základních zásad ochrany osobních údajů) považovat za oprávněné, nicméně použití softwaru keylogging bude pro kontrolu zaměstnanců, především pokud zaměstnavatel nemá důvodné podezření např. ze spáchání trestného činu, nepřiměřené.

V zásadě lze říci, že pokud zaměstnavatel zakazuje používání internetu na pracovišti pro osobní účely, může zaměstnavatel legálně provádět namátkové kontroly dat s cílem ověřit, zda zaměstnanci využívají internet pouze pro účely práce. Pro zamezení takového porušování firemních pravidel zaměstnavatele považujeme za velmi efektivní a právně bezvadné řešení zavedení blokace určitých webových stránek či domén např. sociálních sítí, pornografických stránek atd. (tzv. blacklistů) či alternativně taxativní vymezení webových stránek, které určitý zaměstnanec může navštěvovat (tzv. whitelist). Pokud však zaměstnavatel povoluje nebo toleruje používání internetu pro osobní účely, musí získat individuální souhlas zaměstnanců s jakýmkoli plánovaným sledováním, které musí zahrnovat typ a rozsah monitorování.

Jiným případem je monitoring vystupování zaměstnance na sociálních sítích a posouzení, zda takové jednání může být důvodem pro skončení pracovního poměru. Domníváme se, že zaměstnavatel by neměl dlouhodobě sledovat chování zaměstnance na sociálních sítích. Ze zahraniční judikatury lze zmínit např. rozsudek pracovního soudu v Mannheimu ze dne 19. února 2016, sp. zn. 6 Ca 190/15, ve kterém soud rozhodl, že okamžité zrušení pracovního poměru zaměstnance, strojvedoucího vlaku, který vyjadřoval rasistické názory prostřednictvím videa natočeného během pracovní doby v pracovním oděvu, uveřejněného na svém facebookovém profilu, bylo oprávněné. Ve světle vývoje zahraniční judikatury[8] se přikláníme k závěru, že český zaměstnavatel může při důvodném podezření provádět kontroly chování svých zaměstnanců na sociálních sítí a může z výsledků těchto kontrol vyvozovat pracovněprávní důsledky, které mohou v některých případech představovat i důvod pro okamžité zrušení pracovního poměru.

Závěr první části

Zákonnost jakéhokoli druhu monitoringu zaměstnance bude vždy záležet na dodržení základních

zásad pro zachování ochrany soukromí zaměstnance (zásada proporcionality, zásada legitimity a zásada legality, ale také zásada rovného zacházení) a obecných povinností zaměstnavatele. Obecně platí, že zaměstnavatel musí zaměstnance o způsobu a rozsahu monitoringu předem informovat. Rozsah prováděné kontroly by měl být omezený a přiměřený tak, aby odpovídal sledovanému účelu a cíli kontroly. Zaměstnavatel by měl pří dosažení účelu kontroly zároveň zvolit takové metody, které budou pro dosažení požadovaného účelu co nejméně invazivní a získané výsledky využít pouze k původnímu účelu.

"*Toto je první část dvoudílného článku Monitoring činností zaměstnanců ze strany zaměstnavatele. Druhá část bude věnována dalším způsobům monitoringu zaměstnanců a sankcím, které zaměstnavateli hrozí v případě, kdy by se uchýlil k nezákonnému monitoringu*."

Mgr. Martin Murad,
advokát

Mgr. Adéla Uhrinová

ROWAN LEGAL, advokátní kancelář s.r.o.

GEMINI Center
Na Pankráci 1683/127
140 00 Praha 4

Tel.: +420 224 216 212
Fax: +420 224 215 823
e-mail: praha@rowanlegal.com

---

[1] Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.
[2] Nařízení evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.
[3] Aktualizováno v únoru 2014.
[4] K dispozici >>> zde.
[5] DLP nástroje řeší problematiku úniku dat způsobenou pochybením lidského faktoru.
[6] Rozhodnutí Nejvyššího soudu České republiky ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011.
[7]Keylogger je druh programu, který snímá a zaznamenává stisky kláves na klávesnici.
[8] Dále například rozsudek pracovního soudu v Herne ze dne 22. 3. 2016 sp. zn. 5 Ca 2806/15.

Další články:

- Odpovědnost zaměstnavatele a zaměstnance v souvislosti s využitím umělé inteligence

- Nový návrh zákona o platformové práci – 2. díl: Redefinice závislé práce
- Home office v Česku, Německu a Rakousku: je česká právní úprava práce na dálku dostatečně flexibilní?
- Postoupení pohledávky na náhradu škody v pracovněprávních vztazích
- Návrh zákona o digitálních platformách přináší více, než se na první pohled zdá
- Odposlechy na pracovišti, policejní vyšetřování a skončení pracovního poměru
- Odpovědnost zaměstnance za schodek
- Konec improvizace v odměňování: zamyšlení nad návrhem transpozice směrnice o transparentním odměňování
- Nový návrh zákona o platformové práci – 1. díl
- Genderový audit jako strategický nástroj zaměstnavatele: Jak se připravit na implementaci směrnice 2023/970?
- Pokuta za švarcsystém kurýrů Rohlíku potvrzena Ústavním soudem