



Monitoring emailových zpráv zaměstnanců

23. 3. 2021

Zdroj: shutterstock.com

Cílem tohoto příspěvku je odpovědět na otázku Jak může zaměstnavatel monitorovat emailové zprávy zaměstnanců? V praxi může zaměstnavatel chtít z různých důvodů monitorovat emaily, jejich tok, obsah a v některých případech emaily zaměstnanců i vyřizovat. Otázka je, zda a za jakých podmínek to právo připouští. Tento článek stručně představuje (I) právní rámec této problematiky, (II) možnosti zaměstnavatele monitorovat a vyřizovat emailové zprávy zaměstnanců, (III) povinnosti zaměstnavatele, (IV) sankce hrozící zaměstnavateli a (V) praktické řešení této problematiky.

Právní rámec

V případě monitoringu emailových zpráv zaměstnanců dochází k prolínání pracovního práva, zejména zák. č. [262/2006](#) Sb., zákoník práce („**ZP**“), s právem na ochranu osobních údajů, zejména nařízení (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů („**GDPR**“). Podpůrně se použije rovněž zák. č. [89/2012](#) Sb., občanský zákoník („**OZ**“), který upravuje právo na ochranu soukromí a majetková práva. Právě ty zde kolidují. Jejich kolize v závislosti na konkrétních okolnostech ve výsledku určuje, zda a za jakých podmínek je možný monitoring a vyřizování emailových zpráv zaměstnanců.

Kolidující práva jsou navíc zaručena ústavním právem a mezinárodními dohodami. Právo na soukromí je zaručeno čl. 8 Úmluvy o ochraně lidských práv a svobod („**Úmluva**“) a čl. 10, 12 a v tomto kontextu důležitým čl. 13 ústavního zák. č. [2/1993](#) Sb., Listiny základních práv a svobod („**Listina**“). Majetkové zájmy, v tomto kontextu zaměstnavatele, jsou zaručeny v čl. 1 dodatkového protokolu č. 1 k Úmluvě a čl. 11 a 26 Listiny.

Dle konstantní judikatury jsou emailové zprávy zaměstnance součástí práva na soukromí a spadají pod ochranu dle čl. 8 Úmluvy.[\[1\]](#) A to i tehdy, když jsou odesílány z pracoviště, v pracovní době, z pracovního počítače a pracovního účtu. Úmluva totiž nerozlišuje mezi osobní a pracovní korespondencí.[\[2\]](#) Totéž platí o čl. 13 Listiny.[\[3\]](#) Tato ochrana soukromí zaměstnance potom může v praxi některým zaměstnavatelům činit potíže, neboť mimo jiné znamená, že monitoring a vyřizování emailových zpráv zaměstnanců je možný pouze způsobem stanoveným v zákoně a za použití testu proporcionality.

Není monitoring, jako monitoring

Předně je nutné rozlišit, zda jde o zařízení případně účet zaměstnance či zaměstnavatele a pokud zaměstnavatele, tak zda má zaměstnanec výslovně povoleno používat je pro soukromé účely. Této problematice se věnujeme v jiném článku.[\[4\]](#) Ve zkratce: jde-li o zařízení či účet zaměstnavatele a platí-li zákaz používat jej pro soukromé účely, lze přiměřeně monitorovat pouze tok emailových zpráv za účelem kontroly dodržování zákazu.

Dále je nutné odlišit situace, ve kterých je monitoring dán závažným důvodem spočívajícím ve zvláštní povaze činnosti zaměstnavatele. I tím se zabýváme v jiném článku.[\[5\]](#) Ve zkratce: monitorovat emailové zprávy lze, pokud je takový důvod skutečně dán a pokud jsou splněny další zákonem předepsané podmínky. Povaha monitorování a jeho rozsah bude záviset na konkrétních okolnostech. V těchto případech důrazně doporučujeme konzultaci s odborníky.

Co však dělat v situaci, kdy není ani jedna z těchto variant možná či dostatečná? Jde například o situaci, kdy zaměstnanec je nemocný a pracovní emaily nevyřizuje, nicméně zaměstnavatel jejich vyřízení potřebuje a rád by je za zaměstnance vyřídil. V takové situaci lze k problematice přistoupit analogicky, jako k problematice listinné pošty zasílané na adresu zaměstnavatele.[\[6\]](#)

Nejprve je nutné analyzovat formát emailové adresy. Obecná adresa typu „*info@firma.cz*“ je adresou zaměstnavatele. Právo na listovní tajemství zde chrání zaměstnavatele. Zaměstnavatel může takovou adresu v zásadě libovolně monitorovat včetně obsahu a vyřizovat jednotlivé zprávy i za situace, kdy je nakládání s touto adresou svěřeno jedinému zaměstnanci např. podatelny.[\[7\]](#) Výjimkou je situace, kdy i na takovou adresu bude doručena zpráva zjevně soukromé povahy, což lze určit na základě dalších identifikátorů jako je odesílatel, předmět či oslovení adresáta.[\[8\]](#)

Adresa typu „*jméno@firma.cz*“ je pak adresa konkrétního zaměstnance a právo na listovní tajemství svědčí jemu. Neznamená to sice, že by ji zaměstnavatel nemohl za žádných okolností kontrolovat, ovšem riziko, že monitoring naruší soukromí zaměstnance se zvyšuje, neboť formát adresy zvyšuje možnost, že zpráva bude soukromého charakteru.[\[9\]](#) Je tedy nutné obezřetně zkoumat další identifikátory takové zprávy (odesílatel, předmět, oslovení).[\[10\]](#) Monitoring těchto zpráv musí být primárně omezen na jejich tok, nikoliv obsah.[\[11\]](#) I zde ovšem existuje výjimka. Zaměstnavatel může sledovat obsah emailových zpráv doručovaných na takovou adresu a některé tyto zprávy vyřídít, pokud (i) na základě analýzy identifikátorů zprávy dospěje k závěru, že nejde o ryze soukromou zprávu, a zároveň (ii) takové jednání projde testem proporcionality.[\[12\]](#)

Test proporcionality je obecně definován kumulativními podmínkami (i) legitimacy, (ii) vhodnosti, (iii) potřebnosti a (iv) přiměřenosti.[\[13\]](#) Jinými slovy, jednání zasahující do jednoho základního práva (v tomto kontextu soukromí zaměstnance) musí být (i) vedené legitimním zájmem na ochraně jiného základního práva (v tomto kontextu vlastnictví a podnikání zaměstnavatele), (ii) vhodné k dosažení ochrany tohoto jiného práva, (iii) ochrany nelze dosáhnout méně invazivním způsobem, (iv) jiné základní právo v daném kontextu hodnotově převažuje nad původním.

Ve vztahu ke sledování elektronické komunikace zaměstnanců pak tento test judikatura dále rozpracovala a požaduje, aby bylo zkoumáno, zda (i) byl zaměstnanec o možnosti monitorování předem informován, (ii) měl zaměstnavatel legitimní důvody ospravedlňující monitorování a zjišťování obsahu zpráv, (iii) mohl zaměstnavatel uplatnit méně invazivní zásah do soukromí zaměstnance, (iv) měl zaměstnanec k dispozici adekvátní záruky (např. zaměstnavatel mohl sledovat obsah komunikace jen po výslovném předchozím upozornění zaměstnance) a dále jaký (v) byl rozsah monitorování a stupeň zásahu do soukromí zaměstnance (např. pouze tok či rovnou obsah zpráv), (vi) byl konečný dopad monitorování na zaměstnance.[\[14\]](#)

Zaměstnavatel tedy může otevřít a vyřídít emailové zprávy doručené na emailovou adresu konkrétního zaměstnance jen (i) ve výjimečných případech,[\[15\]](#) (ii) v zájmu ochrany svých práv, (iii) je-li zřejmé z identifikačních údajů zprávy, že nejde o

soukromou zprávu, (iv) je-li z objektivních důvodů pravděpodobné, že by zaměstnanec zprávu vyřídil pozdě a zaměstnavatel tak utrpěl újmu na svých právech, [\[16\]](#) (v) zaměstnavatel nemá k dispozici méně invazivní řešení, (vi) zaměstnanec byl o postupu zaměstnavatele předem informován a (vii) dopady na zaměstnance nebudou nepřiměřeně negativní. [\[17\]](#) Každý případ je nutné posuzovat v kontextu konkrétních okolností.

Práva a povinnosti zaměstnavatele

Zaměstnavatele má primárně výše uvedené povinnosti identifikace zákonného důvodu monitoringu, analýzy identifikátorů zprávy, provedení testu proporcionality a splnění jeho podmínek, jakož i podmínek daného zákonného důvodu monitoringu. Pokud by se při vyřizování zprávy ukázalo, že navzdory jednotlivým identifikátorům se jedná o soukromou zprávu, je zaměstnavatel povinen čtení a vyřizování takové zprávy okamžitě ukončit. [\[18\]](#)

Dále má zaměstnavatel povinnosti podle GDPR. Tyto povinnosti podrobněji rozebíráme v jiném článku. [\[19\]](#)

Sankce hrozící zaměstnavateli

Za nedodržení povinností hrozí zaměstnavateli sankce, a to jak veřejnoprávní, tak soukromoprávní. Z veřejnoprávních sankcí to je především sankce ve výši až 1.000.000,- Kč za přestupek na úseku ochrany soukromí a osobních práv zaměstnanců. [\[20\]](#) Za porušení povinností podle GDPR potom hrozí sankce ve výši až 20.000.000,- EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obrátu celosvětově za předchozí finanční rok, podle toho, co je vyšší. [\[21\]](#) V extrémních případech může být zaměstnavatel odpovědný i za trestný čin proti právům na ochranu osobnosti, soukromí a listovního tajemství. [\[22\]](#)

Ze soukromoprávních sankcí potom hrozí zaměstnavateli zejména povinnost nahradit zaměstnanci nemajetkovou újmu. Teoreticky může zaměstnavateli vzniknout i povinnost k náhradě majetkové újmy, ušlého zisku a vrácení bezdůvodného obohacení, ovšem v daném kontextu se takový případ prakticky spíše neobjeví. Zároveň může mít zaměstnavatel povinnost ukončit protiprávní monitorování, čtení a vyřizování emailů zaměstnance a do budoucna se zdržet takového jednání.

V případě, že výsledky monitorování či dokonce obsah emailů bude chtít zaměstnavatel použít v řízení proti zaměstnanci, hrozí, že soud takový důkaz neprovede, pokud byl pořízen v rozporu s právními předpisy a jehož pořízením došlo k porušení práv zaměstnance. [\[23\]](#) Jinými slovy, pokud zaměstnavatel při monitorování emailů a jejich obsahu nedodržel výše rozebrané povinnosti, nemusí být důkaz takovým emailem proveden.

Závěr, aneb praktické řešení

Při monitoringu a vyřizování pracovních emailů zaměstnanců zaměstnavatelem je nutné postupovat obezřetně, neboť zde dochází ke kolizi dvou základních práv – práva zaměstnance na soukromí s vlastnickým právem a svobodou podnikání zaměstnavatele. Zákon i judikatura proto kladou striktní podmínky na takové jednání zaměstnavatele. Za splnění těchto podmínek pak zaměstnavatel může přistoupit nejen k monitoringu, ale i k vyřizování emailových zpráv zaměstnanců.

Zaměstnavatelům doporučujeme provést analýzu (i) své činnosti a relevantních procesů, (ii) fungování zaměstnanců v oblasti IT, (iii) důvodů, pro které se může reakce zaměstnance na určitou emailovou zprávu zpozdít, (iv) hrozeb na své i zaměstnancově straně pro případ pozdních reakcí zaměstnanců na určité emailové zprávy i pro případ narušení soukromí těchto emailových zpráv, a to v kontextu jednotlivých důvodů a (v) vhodných a co nejméně invazivních řešení.

Výsledky takové analýzy doporučujeme promítnout do vnitřního předpisu, který musí ochránit zájmy zaměstnance i zaměstnavatele a vyhovět právním předpisům, tedy zejména ZP a GDPR. Do zpracování takového vnitřního předpisu doporučujeme zapojit příslušná interní oddělení i externí odborníky na pracovní právo a právo IT/IP. Nakonec je nutné zaměstnance s takovým vnitřním předpisem řádně a prokazatelně seznámit.

Mgr. Karin Pomaizlová
Mgr. Radim Doležal