Časopis výzkumu a aplikací v profesionální bezpečnosti (JOSRA). JOSRA 2-3 - 2020, roč. 13.

Rakouská úprava užívání Internetu ze strany zaměstnance a limity kontroly ze strany zaměstnavatele

19.11.2020

INTERNET USAGE OF EMPLOYEES AND THE LIMITS OF CONTROL IN AUSTRIAN LAW

Harald Christian Scheu

Právnická fakulta Univerzity Karlovy, scheu@prf.cuni.cz

pracoviště kontrola ochrana osobních údajů GDPR internet

Abstrakt

Ten příspěvek obsahuje analýzu rakouského přístupu k problému sledování soukromého užívání internetu ze strany zaměstnanců a vymezuje právní limity pro zaměstnavatele, který chce soukromé užívání internetu na pracovišti kontrolovat a omezovat. Jako hlavní referenční rámec slouží přitom rakouská a evropská úprava ochrany osobních údajů.

Klíčová slova: soukromé užívání internetu, pracoviště, kontrola, ochrana osobních údajů, zásada proporcionality, GDPR

Abstract

This paper contains an analysis of the Austrian approach to the problem of monitoring private internet usage of employees and defines legal limits for employers who want to control and limit private internet use in the workplace. Austrian and European data protection law serves as the major point of reference.

Keywords: private use of the internet, workplace, control, protection of personal data, principle of proportionality, GDPR

Přijat k publikování / Received for publication 31. 8. 2020

Tento příspěvek vznikl díky finanční podpoře poskytované v rámci výzkumného projektu „Pracovněprávní vztahy a BOZP v kontextu kontroly povinností vyplývajících z § 316 zákoníku práce“, identifikační list potřeby č. V07-S4 VÚBP.

Úvod

Již v období před koronavirovou krizí a hromadným přechodem mnoha podniků do režimu home office platilo, že prakticky každé pracovní místo kancelářského typu mělo přístup k internetu. Jelikož zaměstnavatel má zpravidla zájem o to, aby pracovní doba zaměstnanců byla využita efektivně, je třeba položit otázku, za jakých podmínek mohou zaměstnanci během pracovní doby užívat internet pro soukromé účely a do jaké míry a popř. jakými způsoby může zaměstnavatel užívání internetu ze strany zaměstnanců kontrolovat.

Ačkoli GDPR stanoví určitý společný rámec pro všechny členské státy EU, lze zkoumat a porovnat různé národní přístupy k ochraně osobních údajů na pracovišti. V tomto krátkém příspěvku se chceme zaměřit na otázku, jak rakouská úprava a právní praxe přistupuje k problému sledování chování zaměstnanců v kybernetickém prostoru. Jaké limity stanoví rakouské právo ochrany osobních údajů snaze zaměstnavatelů o kontrolu užívání internetu?

Právní základy rakouské úpravy užívání internetu ze strany zaměstnanců

Rakouská úprava ochrany osobních údajů na pracovišti se skládá ze tří normativních rovin. Kromě obecné úpravy ochrany osobních údajů, která se zakládá především z GDPR[1] a navazujícím zákoně o ochraně osobních údajů z roku 2000 ve znění podle dvou zákonů z let 2017 a 2018,[2] je třeba brát v potaz kolektivní podnikové statuty (*Betriebsverfassung*) a individuální pracovní právo.

Je však třeba říct, že obecné normy explicitně neupravují otázku, za jakých podmínek a do jaké míry má zaměstnanec právo na užívání internetu na pracovišti. Jako výjimku lze uvést § 79d rakouského služebního zákona,[3] který stanoví, že státní úředníci mohou informační a komunikační infrastrukturu zaměstnavatele užívat v zásadě pouze pro služební účely. Podle § 79d služebního zákona je však soukromé využívání této infrastruktury povoleno v omezené míře, pokud nedochází např. ke zneužívání, k poškození pověsti veřejné služby či narušení řádné služby. Citovaná norma dále odkazuje na případná nařízení spolkové vlády, které mohou používání informačních a komunikačních technologií pro soukromé účely nebo na pracovišti podrobněji upravit, zejména co se týká časového rámce, rozsahu a typu povoleného soukromého používání informační a komunikační infrastruktury. Pro oblast mimo veřejnou službu mohou být pravidla užívání internetu upravena v individuální pracovní smlouvě či v kolektivním podnikovém statutu.

Odborná doktrína vychází z toho, že pokud není upraveno jinak, lze užívání internetu na pracovišti považovat za povolené v rozumné a přiměřené míře. To zahrnuje standardně např. stahování souborů a odesílání emailů.[4] Zaměstnanec přitom však za žádných okolností nesmí zanedbávat pracovní povinnosti nebo narušit fungování pracoviště. Návštěva zpoplatněných stránek nebo nevhodných stránek, tzn např. stránek s pornografickým či politicky extremistickým obsahem není bez výslovného svolení ze strany zaměstnavatele povolena.[5] Podle Wolfganga Goricnika, právního odborníka rakouské Komory zaměstnanců (Arbeiterkammer), však není na pracovišti zakázáno ani prohlížení pornografických stránek, protože pracovní právo nemá sloužit jako morální instance. Goricnik ovšem připouští, že zaměstnavatel může technicky zamezit přístup k takovým stránkám, jelikož zaměstnanec na druhé straně samozřejmě ani nemá právo na přístup k pornografickým stránkám na pracovišti.[6]

Odborná literatura vnímá užívání internetu pro soukromé účely v rozsahu 15-20 minut za den za běžný a přípustný standard (ve vztahu k osmihodinovému pracovnímu dni),[7] byť v konkrétních případech může být tato doba kratší, ale také delší. V rozsudku ze září 2009 Nejvyšší soud ve Vídni řešil případ zaměstnance, který pravidelně strávil soukromým surfováním po internetu a stahováním rozsáhlých filmových a hudebních souborů alespoň jednu a půl hodiny denně z pracovní doby. Podle Nejvyššího soudu zaměstnanec ztratil důvěru zaměstnavatele a jeho propuštění ze zaměstnání bylo proto v souladu s právem, a to bez ohledu na to, zda k užívání internetu došlo částečně během pracovní přestávky. Nejvyšší soud dodal, že při propuštění kvůli nadměrnému užívání internetu na pracovišti není ani rozhodující případný úmysl zaměstnance poškodit zájmy zaměstnavatele nebo otázka, zda ke škodě skutečně došlo.

Bylo považováno za dostačující, že si zaměstnanec uvědomil, že jednal v rozporu se svými pracovními povinnostmi.[8]

Vzhledem k tomu, že užívání internetu na pracovišti je tedy v určité míře povoleno, může nastat problematická situace, že v rámci informačního systému jsou společně ukládány obchodní a soukromá data. Pokud zaměstnavatel přistupuje ke svým obchodním údajům, může narazit na soukromé údaje svých zaměstnanců. Pomocí monitorování těchto údajů by mohl detailně kontrolovat užívání internetu ze strany zaměstnance. Právo stanoví zaměstnavateli však konkrétní limity.

Limity kontroly ze strany zaměstnavatele

Z právního hlediska je nepřípustné užívání spyware, tzn. sledovacího softwaru, který odesílá data z počítače bez vědomí zaměstnance. Rakouská doktrína považuje skryté sledování zaměstnance v každém případě za zásah do jeho lidské důstojnosti. Na této kvalifikaci nemění nic ani případný souhlas podnikové rady (Betriebsrat). Užívání spyware je protiprávní i v případě, že by se zaměstnanec dopustil nepovoleného užívání internetu na pracovišti.

Tyto závěry lze opřít o čl. 5 odst. 1a) GDPR, podle něhož osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem. Uvedený postup zaměstnavatele je z tohoto hlediska v jednoznačném rozporu se zásadou transparentnosti. Skryté užívání spyware by bylo zřejmě také v rozporu s informačními povinnosti upravenými v čl. 13 a 14 GDPR.

V absenci konkrétní rakouské judikatury na toto téma lze odkázat na rozsudek německého Spolkového pracovního soudu ze dne 27. července 2017,[9] ve kterém bylo za protiprávní označeno používání softwarového keyloggeru, s nímž byly skrytě zaznamenávány všechny vstupy do klávesnice na firemním počítači za účelem kontroly zaměstnance. Poté, co zaměstnavatel nainstaloval do pracovního počítače zaměstnance softwarový keylogger, který zaznamenával všechny stisky kláves a pravidelně pořizoval snímky obrazovky, zjistil, že zaměstnanec vykonal na pracovišti značné množství soukromé práce a ukončil s ním pracovní poměr. Podle Spolkového pracovního soudu byly však informace získané pomocí spyware zcela nepoužitelné v následujícím soudním sporu.[10]

Protiprávní je také čtení obsahu soukromých emailů zaměstnanců, a to i v případě, že by zaměstnavatel explicitně zakázal užívání firemní emailové schránky pro soukromé účely. Rakouská doktrína se v této souvislosti opírá o ustanovení § 16 Všeobecného zákoníku občanského (ABGB), podle něhož „každý člověk má vrozená, již rozumem poznatelná práva, a nutno jej tudíž považovati za osobu“. Obecný rámec § 16 ABGB je konkretizován v § 93 odst. 3 zákona o telekomunikaci,[11] který zakazuje odposlouchávání, zaznamenávání, zachycování nebo jiné sledování zpráv a souvisejících provozních a lokalizačních údajů, jakož i zveřejňování informací o nich osobami jinými než uživatel bez souhlasu všech zúčastněných uživatelů.[12]

Odborníci na pracovní právo doporučují výslovnou úpravu podmínek, za kterých zaměstnanec může užívat firemní infrastrukturu pro soukromé emaily.[13] Určitý rámec stanoví v tomto směru § 96 odst. 1 zákona upravujícího kolektivní vyjednávání,[14] podle něhož zavedení kontrolních opatření a technických systémů pro kontrolu zaměstnanců vyžaduje souhlas ze strany podnikové rady, pokud tato opatření zaměstnavatele mají dopad na lidskou důstojnost zaměstnance. Pokud nebyla zřízena podniková rada, musí s kontrolním opatřením souhlasit každý zaměstnanec individuálně. To vyplývá z § 10 zákona o úpravě právních předpisů v oblasti pracovních smluv,[15] který stanoví, že zavádění a používání kontrolních opatření a technických systémů, které mají vliv na lidskou důstojnost, je povoleno pouze na základě kolektivní smlouvy ve smyslu § 96 odst. 1 zákona upravujícího kolektivní vyjednávání nebo na základě souhlasu zaměstnance, a to v podnicích, v nichž nebyla zřízena podniková rada. Souhlas zaměstnance může být podle § 10 odst. 2 zákona o úpravě právních předpisů v oblasti pracovních smluv kdykoli odvolán bez dodržení výpovědní lhůty.

V této souvislosti je ovšem třeba dbát na to, aby souhlas s omezením ochrany osobnosti zaměstnance nebyl v rozporu s dobrými mravy. Ačkoli osobnostní práva zaměstnance mohou být do určité míry předmětem ujednání mezi zaměstnavatelem a zaměstnancem, nelze přehlédnout nerovný poměr mezi oběma stranami a skutečnost, že zaměstnanec je ekonomicky závislý na zaměstnavateli. Odborná doktrína hovoří o tzv. „zředěné svobodě vůli“ (*vedünnte Willensfreiheit*) a předpokládá, že souhlas zaměstnance s nepřiměřenými kontrolními opatřeními je podle § 879 odst. 1 ABGB neplatný.[16]

V tomto směru bude vykládán také čl. 4 odst. 11 GDPR, podle něhož se „souhlasem“ subjektu údajů rozumí jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Při zpracování zvláštních kategorií osobních údajů navíc platí podle čl. 9 odst. 2 GDPR, že subjekt údajů musí udělit výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz nemůže být subjektem údajů zrušen. Ve smyslu čl. 5 odst. 1 GDPR musí být zaměstnanec plně informován o procesu zpracování údajů a době trvání ukládání údajů. Souhlas s nepřiměřenými kontrolními opatřeními by byl tedy i z tohoto hlediska neplatný.[17]

Odborníci doporučují, aby ujednání mezi zaměstnavatelem a zaměstnancem obsahovalo též úpravu otázky přístupu jiných zaměstnanců do emailové schránky zaměstnance po dobu jeho delší nepřítomnosti na pracovišti např. z důvodu nemoci. Kontrola emailové schránky by měla být provedena za přítomnosti pověřeného člena podnikové rady nebo podnikového zmocněnce pro ochranu osobních údajů.[18]

Model třístupňové kontroly

Již v roce 2004 představila tehdejší zmocněnkyně Rady Evropy pro ochranu osobních údajů Waltraud Kotschy spolu se Sebastianem Reimerem model založený na třech stupních kontroly ze strany zaměstnavatele.[19] První rovinu kontroly představuje automatizovaný dohled nad zajištěním funkčnosti systému, druhou rovinu zjištění výrazných odchylek od standardního užívání komunikační infrastruktury a poslední stupeň kontrola konkrétních komunikačních údajů v případě podezření z porušení práva (např. pracovní smlouvy).

Automatizovaný dohled zahrnuje opatření proti počítačovým virům a jiným útokům neoprávněných osob na systém. Je zřejmé, že v této fázi zaměstnavatel nemůže rozlišit mezi firemní a soukromou komunikací. Oba způsoby komunikace mohou totiž ohrožovat funkčnost systému ve stejné míře. Zajištění této fáze kontroly je zpravidla v rukou administrátorů komunikačního systému. Ti mohou např. blokovat zprávy s podezřelými a nebezpečnými přílohami a informovat o tom příjemce zprávy.

Až na druhém stupni může administrátor zjistit, od kterého konkrétního zaměstnance vychází specifické riziko pro funkčnost IT systému. Tato kontrola může identifikovat zaměstnance, který stahuje příliš rozsáhlé soubory nebo přijímá zprávy s problematickými přílohami. Opatření přijatá v rámci druhého stupně kontroly představují zpracování osobních údajů, pro které čl. 13 GDPR dnes předpokládá, že zaměstnanec bude informován. Jelikož hlavní podíl na praktickém provedení druhé roviny kontroly má IT oddělení, je také na místě zajistit mlčenlivost administrátorů. Thomas Hartmann v této souvislosti přirovnal postavení IT oddělení k černé skříně (*black box*) a vyjádřil naději, že zaměstnavatelé budou dodržovat požadavky na integritu správce systému.[20]

Souhru první a druhé roviny kontroly dokumentuje Wolfgang Goricnik pomocí jednoduchého příkladu. Zaměstnanec instaloval na svém pracovním počítači prvky, které reprodukovaly obrazy živé kamery monitorující vodní díru v poušti Kalahari, kam dotyčný zaměstnanec zřejmě zavítal během dovolené. Přiměřené užívání firemní komunikační infrastruktury bylo zaměstnavatelem povoleno, a občasné prohlížení obrazů živé kamery zřejmě nemohlo negativně

ovlivnit pracovní výkon zaměstnance. Problém spočítal v tom, že neustálým stahováním velkého množství dat byla narušena funkčnost IT systému. Poté, co IT oddělení na základě komunikace se zaměstnancem zjistila původ problému, byl prvek odstraněn. Podstatné přitom je, že se o problému a jeho odstranění zaměstnavatel vůbec nemusel dozvědět. [21]

Až ve třetí fázi kontroly je jméno zaměstnance předáno zaměstnavateli, přičemž informována má být také podniková rada a člen podnikové rady se má také zúčastnit pohovoru zaměstnavatele se zaměstnancem.[22] První a druhý stupeň kontroly lze podle doktríny přeskočit pouze v případě bezprostředního nebezpečí pro komunikační systém zaměstnavatele nebo v případě podezření ze spáchání trestného činu. Podle čl. 5 odst. 1 a čl. 13 GDPR však musí být zaměstnanec informován také v těchto výjimečných případech.[23] Wolfgang Goricnik se domnívá, že by zaměstnavatel mohl v uvedených případech nařídit také skrytý postup, ale vždy za dodržování zásady proporcionality. Získaná data by byla použitelná pouze v rámci soudního řízení a musela by být ihned vymazána po pravomocném ukončení řízení.[24]

Zde popsaný model třístupňové kontroly tedy poskytuje zaměstnavateli určitý návod, jak správně zohlednit zásadu proporcionality při užívání kontrolních nástrojů. V zásadě ladí tento model také s doporučeními pracovní skupiny pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů,[25] která ve svém stanovisku z června 2017[26] zdůraznila, že monitorování všech online aktivit zaměstnanců je zpravidla nepřiměřeným opatřením a že monitorování by mělo vždy být prováděno jen v nutném rozsahu.[27]

Jelikož Evropská úmluva o ochraně lidských práv a základních svobod tvoří integrální součást rakouského ústavního pořádku, je třeba dbát též na dodržování standardů určeného Evropským soudem pro lidská práva. Když Velký senát ESLP řešil v případě Barbulescu v. Rumunsko[28] problém sledování soukromých chatových zpráv zaměstnance ze strany zaměstnavatele, stanovil několik zásad, které mají smluvní strany respektovat. Ve světle zásady proporcionality má být podle ESLP zohledněno:

- zda byl pracovník před dozorem informován o tom, že by jeho komunikace mohla být sledována,
- rozsah dozoru a narušení soukromí (zejména zda je obsah komunikace také ukládán),
- zda měl zaměstnavatel dostatečné důvody ke sledování komunikace a přečtení obsahu,
- jaké jsou důsledky systému sledování zpráv a jak je zaměstnavatelem využit,
- zda existují přiměřené ochranné mechanismy, které zajišťují, aby zaměstnavatel nemohl vzít na vědomí obsah zpráv, dokud zaměstnanec nebyl o této možnosti informován.

Lze dodat, že model navržený autory Kotschy a Reimerem rezonuje nejen v odborné literatuře,[29] ale také v judikatuře rakouských soudů.[30]

Závěr

V tomto článku jsme se věnovali rakouském přístupu k problému sledování chování zaměstnanců v kybernetickém prostoru. V první části článku jsme analyzovali kritéria užívání internetu pro soukromé účely na pracovišti. Dále jsme vymezili limity, které rakouské právo stanoví zaměstnavatelům, kteří usilují o kontrolu užívání internetu ze strany zaměstnanců. Jelikož relevantní právní normy až na zmíněné výjimky neupravují užívání internetu na pracovišti explicitně, je nutné konkrétní právní rámec odvozovat především z principů obsažených v rakouské ústavě včetně Evropské úmluvy o lidských právech, v GDPR a ve vnitrostátních zákonech. Právní praxe potvrzuje, že není vždy jednoduché správně vybalancovat zájmy zaměstnavatele a zaměstnance ve světle principu proporcionality.

Příslušná právní dogmatika, která byla rakouskou judikaturou a doktrínou zformulována ještě před účinností GDPR, z velké části přetrvává i v nových podmínkách. V zájmu právní jistoty odborníci na ochranu osobních údajů doporučují stanovení jasných interních pravidel v rámci tzv. *internet privacy policy*. Rakouská doktrína v tomto směru ladí s výše

citovaným stanoviskem pracovní skupiny zřízené podle čl. 29,[31] které požaduje, aby zaměstnavatelé uplatňovali pravidla přijatelného používání spolu s pravidly na ochranu soukromí (privacy policies), přičemž mají popisovat přípustné používání sítě a vybavení organizace a mají důrazně a podrobně uvést, k jakému zpracování dochází.

Lze dodat, že jasná pravidla budou velmi potřebná také v případě obnovení režimu home office pro mnoho zaměstnanců v důsledku případných dalších koronavirových vln.

Použitá literatura

GRÜNANGER, Josef; GORICNIK, WolfganG. *Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle*. Wien: MANZ Verlag, 2018. S. 240.

HARTMANN, Thomas. Die Beamten-Dienstrechtsnovelle als Modell für die Nutzung und Kontrolle von Internet am Arbeitsplatz? *JusIT*. 2010, Nr. 2, s. 50.

KOTSCHY, W.; REIMER, S. Die Überwachung der Internet-Kommunikation am Arbeitsplatz: ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht. *Zeitschrift für Arbeitsrecht und Sozialrecht*. 2004, Nr. 29, s. 169.

KRAFT, Rainer. In flagranti im Internet. *Jusclub.* 2007, Nr. 3, s. 13.

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 (obecné nařízení o ochraně osobních údajů).

Vzorová citace

SCHEU, Harald Christian. Rakouská úprava užívání Internetu ze strany zaměstnance a limity kontroly ze strany zaměstnavatele. *Časopis výzkumu a aplikací v profesionální bezpečnosti* [online]. 2020, roč. 13, č. 2-3. Dostupný z: https://www.bozpinfo.cz/josra/rakouska-uprava-uzivani-internetu-ze-strany-zamestnance-limity-kontroly-ze-strany. ISSN 1803-3687.

1] 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 (obecné nařízení o ochraně osobních údajů).

2] V návaznosti na GDPR byly v Rakousku přijaty adaptační zákon (Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017) a zákon o deregulaci ochrany osobních údajů (Datenschutz-Deregulierungs-Gesetz 2018, BGBl I Nr. 24/2018).

3] Beamten-Dienstrechtsgesetz 1979, BGBl. Nr. 333/1979.

4] V rozsudku ze dne 7. 5. 2003 Vrchní soud ve Vídni přirovnal tuto rozumnou míru užívání internetu k soukromým telefonickým hovorům z pracoviště. Viz OLG Wien 7. 5. 2003, 8 Ra 45/03a.

5] Kraft, Rainer. In flagranti im Internet. *Jusclub,* 3/2007, str. 13.

6] Grünanger/Goricnik (eds.) Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle. Wien, 2018, str. 240.

7] Viz např. Ruß, Verena. Glosse zu OGH 29. 9. 2011, ObA 52/11x, jusIT, 2012/5, str. 12.

8] 8ObA52/11x.

9] 2 AZR 681/16.

10] Zbývá ovšem dodat, že podle německé doktríny může být skryté nasazení spyware přípustné, pokud v daném případě existují náznaky podezření na trestný čin nebo porušení povinnosti v pracovním poměru. Protiprávní je tedy pouze nepřetržité monitorování bez příčiny a bez konkrétních důkazů. Podrobněji Oberthür, Nathalie. Der Einsatz von Keyloggern am Dienst-PC – keine anlasslose Dauerüberwachung am Arbeitsplatz. Juris, 3/2018, str. 106. Německá doktrína nerevidovala tuto interpretaci ani po vstupu GDPR v účinnost. Viz např. komentář Nicolaie Besgena „Keylogger und Arbeitnehmerdatenschutz“ ze dne 25. 10. 2018 na stránkách advokátní kanceláře Meyer-Köring (https://www.meyer-koering.de/meldungen/3529).

11] Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I Nr. 70/2003.

12] Viz podrobněji Grünanger/Goricnik (eds.) Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle. Wien, 2018, str. 256.

13] Viz např. doporučení na stránkách rakouské Hospodářské komory (Wirtschaftskammer): https://www.wko.at/service/ooe/arbeitsrecht-sozialrecht/Internet-und-E-Mail-am-Arbeitsplatz---welche-Kontrollmassn.html.

14] Arbeitsverfassungsgesetz 1973 – ArbVG, BGBl. Nr. 22/1974.

15] Arbeitsvertragsrechts-Anpassungsgesetz – AVRAG, BGBl. Nr. 459/1993.

16] Ustanovení § 879 odst. 1 ABGB zní: „Smlouva, jež se příčí zákonnému zákazu nebo dobrým mravům, jest neplatna.“

17] Je třeba dodat, že podle čl. 7 odst. 4 GDPR není souhlas zaměstnance považován za svobodný, pokud je tento souhlas podmínkou prodloužení pracovní smlouvy nebo uzavření nové pracovní smlouvy.

18] Srov. Grünanger/Goricnik (eds.) Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle. Wien, 2018, str. 267.

19] Kotschy, W., Reimer, S. Die Überwachung der Internet-Kommunikation am Arbeitsplatz: Ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht, Zeitschrift für Arbeitsrecht und Sozialrecht, 2004/29, 169.

20] Hartmann, Thomas. Die Beamten-Dienstrechtsnovelle als Modell für die Nutzung und Kontrolle von Internet am Arbeitsplatz? JusIT 2/2010, str. 50.

21] Grünanger/Goricnik (eds.) Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle. Wien, 2018, str. 259.

22] Kotschy, W., Reimer, S. Die Überwachung der Internet-Kommunikation am Arbeitsplatz: Ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht, Zeitschrift für Arbeitsrecht und Sozialrecht, 2004/29, 171.

23] Grünanger/Goricnik (eds.) Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle. Wien, 2018, str. 260.

24] Ibidem, 261.

25] Pracovní skupina zřízená podle článku 29 směrnice 95/46/ES o ochraně o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

26] Opinion 2/2017 on data processing at work.

27] Srov. také Vrbíková, B. Stanovisko Pracovní skupiny 29 k monitorování zaměstnanců na pracovišti i mimo něj (článek je dostupný na stránkách https://www.epravo.cz/top/clanky/stanovisko-pracovni-skupiny-29-k-monito...).

28] Stížnost č. 61496/08, rozsudek Velkého senátu ze dne 5. září 2017.

29] Viz např. Hartmann, Thomas. Die Beamten-Dienstrechtsnovelle als Modell für die Nutzung und Kontrolle von Internet am Arbeitsplatz? JusIT 2/2010, str. 48-53.

30] Viz např. VfGH (Verfassungsgerichtshof) G264/2015, VfGH KR1/2014. VwGH (Verwaltungsgerichtshof) 2011/17/0066, VwGH 2015/04/0011,

31] Opinion 2/2017 on data processing at work.

Autor článku:
doc. Dr. iur. Harald Christian Scheu, Mag. phil., Ph.D.