ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Katedra pracovního práva a práva sociálního zabezpečení

DIPLOMOVÁ PRÁCE

Monitoring zaměstnanců ve světle judikatury ČR

Plzeň, 2022 Kim Ondráčková

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Katedra pracovního práva a práva sociálního zabezpečení

DIPLOMOVÁ PRÁCE

Monitoring zaměstnanců ve světle judikatury ČR

Zpracovala:	Kim Ondráčková
Studijní program:	M6805 Právo a právní věda
Vedoucí diplomové práce:	JUDr. Eva Benešová, LL.M., Ph.D.
Pracoviště:	Katedra pracovního práva a sociálního zabezpečení

Plzeň, 2022

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Kim ONDRÁČKOVÁ**
Osobní číslo:	**R17M0225P**
Studijní program:	**M6805 Právo a právní věda**
Studijní obor:	**Právo**
Téma práce:	**Monitoring zaměstnanců ve světle judikatury České republiky**
Zadávající katedra:	**Katedra pracovního práva a práva sociálního zabezpečení**

Zásady pro vypracování

1. Úvod
2. Právní úprava
3. Formy monitoringu
4. Povinnosti zaměstnavatele ve vztahu k monitoringu
5. Komparace s cizí právní úpravou
6. Závěr

Rozsah diplomové práce:
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná**

Seznam doporučené literatury:

- HUSSEINI, Faisal. Listina základních práv a svobod: komentář. Praha: C.H. Beck, 2021. Beckova edice komentované zákony. ISBN 978-80-7400-812-2.
- BĚLINA, Miroslav. Zákoník práce: komentář. 3. vydání. Praha: C.H. Beck, 2019. Velké komentáře. ISBN 978-80-7400-759-0.
- NULÍČEK, Michal. Zákon o zpracování osobních údajů. Praha: Wolters Kluwer, 2019. Praktický komentář. ISBN 978-80-7598-467-8.
- BĚLINA, Miroslav, PICHRT, Jan. Pracovní právo. 7. doplněné a podstatně přepracované vydání. Praha: C.H. Beck, 2017. Academia iuris (C.H. Beck). ISBN 978-80-7400-667-8.
- BARTÍK, V., JANEČKOVÁ, E. Ochrana osobních údajů v aplikační praxi: (vybrané problémy). 4., aktualizované vydání. Praha: Wolters Kluwer, 2016. Právo prakticky. 304 s. ISBN 978-80-7552-141-5
- JANEČKOVÁ, E., BARTÍK, V. Kamerové systémy v praxi: Právní režim z pohledu ochrany osobních údajů a ochrany osobnosti. Praha: Linde, 2011. 240 s. ISBN 978-80-7201-850-5
- ŠTEFKO, Martin, VYSOKAJOVÁ, Margerita. Personální vademecum. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2016. ISBN 978-80-87975-45-9.
- VIDRNA, Jan, KOUDELKA, Zdeněk. Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců. Praha: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7.

Vedoucí diplomové práce: **JUDr. Eva Benešová, Ph.D., LL.M.**
Katedra pracovního práva a práva sociálního zabezpečení

Datum zadání diplomové práce: **14. března 2021**
Termín odevzdání diplomové práce: **31. března 2022**

Západočeská univerzita v Plzni Fakulta právnická L.S.

JUDr. et PhDr. Stanislav Balík, Ph.D.
děkan

Doc. JUDr. Jarmila Pavlátová, CSc.
vedoucí katedry

V Plzni dne 9. září 2021

Prohlášení

„Prohlašuji, že jsem tuto diplomovou práci zpracovala samostatně, a že jsem vyznačila prameny, z nichž jsem pro svou práci čerpala způsobem ve vědecké práci obvyklým.“

V Plzni dne 31. března 2022

Kim Ondráčková

Poděkování

Na tomto místě bych ráda poděkovala JUDr. Evě Benešové, LL.M., Ph.D. za vedení této diplomové práce, cenné a podnětné rady a připomínky, jakož i čas, který mi věnovala. Mé poděkování patří též mým rodičům, kteří mi byli po celou dobu studia oporou.

Obsah

Úvod ... **1**

1 Právní úprava ... **3**

1. 1 Zákoník práce ... 3

1. 2 Listina základních práv a svobod ... 7

1. 3 Občanský zákoník ... 10

1. 4 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ... 11

1. 5 Zákon o zpracování osobních údajů ... 15

1. 6 Zákon o inspekci práce ... 16

1. 7 Trestní zákoník ... 17

1. 8 Evropská úmluva o ochraně lidských práv a základních svobod ... 18

1. 9 Ostatní prameny ... 19

2 Formy monitoringu ... **22**

2. 1 Monitoring e-mailové schránky ... 22

2. 1. 1 E-mail tvořen osobními údaji zaměstnance ... 23

2. 1. 2 E-mail bez osobních údajů zaměstnance ... 24

2. 1. 3 Doporučení ... 25

2. 1. 4 Rozsudek velkého senátu ESLP ze dne 5. září 2017 ve věci 61496/08 – Bărbulescu proti Rumunsku ... 25

2. 2 Monitoring aktivity zaměstnance na internetu ... 27

2. 2. 1 Doporučení ... 29

2. 2. 2 Monitoring sociálních sítí zaměstnanců ... 29

2. 2. 2 Rozhodnutí Nejvyššího soudu České republiky ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011 ... 32

2. 3 Monitoring firemního telefonu zaměstnance ... 33

2. 3. 1 Rozsudek Nejvyššího soudu ze dne 7. 8. 2014, sp. zn. 21 Cdo 747/2013 ... 35

2. 3. 2 Rozsudek Okresního soudu v Mělníku ze dne 11. 2. 2021, sp. zn. 6 C 306/2019 ... 36

2. 3. 3 Rozsudek ze dne 25. června 1997 ve věci 20605/92 – Halford proti Spojenému království ... 37

2. 3. 4 Nález ÚS České republiky ze dne 9. prosince 2014, sp. zn. II. ÚS 1774/14 ... 37

2. 4 Monitoring prostřednictvím GPS lokalizátorů ... 38

2. 5 Monitoring firemního vozidla, které je zaměstnanci svěřeno k osobním účelům ... 41

2. 5. 1 Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 3. července 2013, sp. zn. UOOU-00237/13 ... 42

2. 5. 2 Rozsudek Městského soudu v Praze ze dne 5. května 2017, sp. zn. 6 A 42/2013 ... 43

2. 6 Kamerové systémy ... 43

2. 6. 1 Rozsudek Městského soudu v Praze ze dne 18. 10. 2016, sp. zn. 5 A 107/2013 ... 46

2. 6. 2 Rozsudek ve věci č. 1874/13 a 8567/13 Lopéz Ribalda a ostatní proti Španělsku ... 48

2. 7 Elektronické docházkové systémy ... 49

2. 8 Povinné testování zaměstnanců na přítomnost viru SARS-CoV-2 (tzv. covid-19) ... 50

2. 8. 1 Rozsudek NSS ze dne 4. března 2022, sp. zn. 5 Ao 31/2021 ... 53

3 Povinnosti zaměstnavatele ve vztahu k monitoringu ... 55

3. 1 Zásada proporcionality ... 55

3. 2 Princip minimalizace údajů ... 57

3. 3 Informační povinnost ... 58

3. 4 Přeshraniční předávání osobních údajů zaměstnanců ... 59

3. 4. 1 Podniková pravidla ... 61

4 Komparace ... 65

4. 1 Finsko ... 65

4. 1. 1 Monitoring zaměstnanců prostřednictvím kamerového systému 66
4. 1. 2 Monitoring e-mailových zpráv zaměstnanců 69
4. 2 Německo 70
4. 2. 1 Monitoring e-mailové adresy a internetové aktivity zaměstnance 75
4. 2. 2 Monitoring prostřednictvím kamerového systému 75
Závěr 79
Resumé 82
Seznam použitých zdrojů 85
Prameny 85
České 85
Cizojazyčné 86
Literatura 87
Česká 87
Cizojazyčná 87
Odborné články 87
České 87
Cizojazyčné 90
Judikatura 90
Česká 90
Cizojazyčná 91
Jiné zdroje 92
České 92
Cizojazyčné 95

Seznam použitých zkratek

ČR	Česká republika
ESLP	Evropský soud pro lidská práva
EU	Evropská unie
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
Listina	Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.
NS	Nejvyšší soud
NSS	Nejvyšší správní soud
ObčZ	Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
SDEU	Soudní dvůr Evropské unie
Směrnice 95/46/ES	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
TZ	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
Úmluva	Sdělení č. 209/1992 Sb., Sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících
ÚOOU	Úřad pro ochranu osobních údajů
ÚS	Ústavní soud České republiky

Ústava	Ústavní zákon č. 1/1993 Sb., Ústava České republiky ve znění pozdějších předpisů
ZP	Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
ZoIP	Zákon č. 251/2005 Sb., zákon o inspekci práce

Úvod

Zaměstnavatelé vždy vyhledávali způsoby, jakými zvýšit efektivitu práce, optimalizovat výrobu, předcházet škodám na majetku či snižovat náklady. Pandemie covid-19 tyto snahy zaměstnavatelů však výrazně umocnila. Mnozí zaměstnavatelé navíc v souvislosti s pandemií zaváděli institut home office. Zaměstnanci tak začali pracovat z domova. Zaměstnavatelům byla v důsledku této změny znesnadněna nejen kontrola pracovní výkonnosti a kvality odvedených pracovních výsledků zaměstnanců, ale též dozor nad majetkem zaměstnavatele, který byl zaměstnancům svěřen. Je proto pochopitelné, že zaměstnavatelé začali vyhledávat mechanismy, jejichž prostřednictvím mohou své zaměstnance sledovat. K tomu jsou využívány častěji než dříve různé prostředky sledování, a to od kamerových systémů po moderní technologie. Problematiku monitoringu je třeba vnímat komplexně. Ekonomické hledisko monitoringu je proto nutné doplnit též o hledisko právní a morální. V souvislosti s využitím sledovacích prostředků vůči zaměstnanci totiž nastává z hlediska práva problém. Důvodem je, že při monitoringu zaměstnanců dochází k zásahu do jejich práva na soukromí. Kromě toho neuváženě zavedený monitoring dokáže během krátkého okamžiku narušit důvěru na pracovišti. V krajních případech tak může zavdat vzniku nepříjemných soudních sporů mezi zaměstnavatelem a zaměstnanci.

Jedním z cílů diplomové práce je poskytnutí uceleného vhledu do zpracovávané problematiky. V práci předestírám ucelený přehled vybraných forem monitoringu. Kromě relevantní právní úpravy v práci čerpám také z dalších zdrojů, a to např. z významných judikátů a odborných článků (českých i zahraničních). Větší pozornost věnuji, dle mého názoru, nejvýznamnějším a nejzajímavějším aspektům této problematiky, kterými jsou přeshraniční předávání osobních údajů zaměstnanců a problematika zpracovávání biometrických údajů. Za další cíl si kladu zodpovězení následujících otázek: Zda je současná právní úprava monitoringu zaměstnanců v právním řádu České republiky dostatečná. V případě, že dospěji k negativnímu závěru, se zaměřím na to, v jaké zahraniční právní úpravě je možné hledat inspiraci. Na základě dosažených zjištění formuluji výsledná doporučení a uvedu, jaké konkrétní změny by měly být přijaty. V neposlední řadě se zabývám otázkou, zda lze považovat monitoring zaměstnanců za otázku spadající ryze do pracovního práva.

Pro zodpovězení těchto otázek nejdříve v první kapitole nastíním právní úpravu monitoringu zaměstnanců. Ve druhé kapitole se zaměřím na jednotlivé formy monitoringu. Vzhledem k pandemii covid-19, která v posledních dvou letech ochromila celý svět, považuji za praktické věnovat v této kapitole prostor též jedné z novodobých forem monitoringu, a to testování zaměstnanců. Po dohodě s vedoucím diplomové práce jsem se proto rozhodla rozšířit výčet forem monitoringu ve druhé kapitole právě o výše uvedený institut. Ve třetí kapitole popíši některé povinnosti, které zaměstnavatelům v souvislosti s monitoringem vznikají. V této kapitole se zaměřím též na přeshraniční předávání osobních údajů zaměstnanců do zahraničí. Přeshraniční předávání údajů považuji v době globalizace a zvýšené mobility zaměstnanců za téma velice aktuální. Čtvrtá kapitola se i z tohoto důvodu věnuje komparativnímu srovnání české právní úpravy s právní úpravou v Německu a ve Finsku. Závěrem shrnu získané poznatky a pokusím se zodpovědět na mnou vytyčené otázky.

V diplomové práci převažuje metoda popisná. Jednotlivé poznatky podrobuji analýze a snažím se z nich formulovat závěry. Ve čtvrté kapitole převažuje metoda komparace.

Cílem mé práce není problematiku monitoringu zaměstnanců vyčerpat. Jedná se o téma rozsáhlé, u kterého lze důvodně předpokládat, že se bude do budoucna zajímavě rozvíjet. Hlavní příčinu dynamického vývoje této problematiky spatřuji v narůstajícím pokroku moderních technologií a zvyšujících se požadavcích, které jsou kladeny na zaměstnance i zaměstnavatele. Ráda bych se proto tímto tématem zabývala i nadále při budoucím bádání.

Diplomová práce vychází z platné právní úpravy ke dni 31. 3. 2022.

1 Právní úprava

Jak jsem již zmínila v úvodu diplomové práce, problematika monitoringu zaměstnanců je poměrně složitým a komplexním tématem. Jedním z hlavních důvodů je roztříštěnost právní úpravy napříč právním řádem České republiky. Dále střet veřejného práva s právem soukromým. Tato kapitola poskytuje nástin primárních pramenů, které jsou pro zpracování tématu monitoringu zaměstnanců klíčové.

1. 1 Zákoník práce

Nejzásadnější právní úpravu monitoringu zaměstnanců představuje zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále také jako „zákoník práce“ nebo „ZP“). Pro poskytnutí lepšího vhledu do problematiky monitorování zaměstnanců považuji za důležité nejdříve charakterizovat vztah mezi zaměstnavatelem a zaměstnancem.

Vztah mezi zaměstnavatelem a zaměstnancem je vztahem nerovným. Zaměstnanec se zde ocitá v postavení podřízeném, zatímco zaměstnavatel v postavení nadřízeném (§ 2 odst. 1 ZP). Dle Úřadu pro ochranu osobních údajů (dále také jako „ÚOOÚ“) lze vztah mezi zaměstnavatelem a zaměstnancem charakterizovat jako vztah alimentačního charakteru. Alimentační charakter má tento vztah proto, neboť je na něm zaměstnanec (mnohdy včetně jeho rodiny) odkázán svým živobytím. Z tohoto důvodu je tento vztah značně právem regulován, a to zpravidla ve prospěch zaměstnance.[1] V pracovním vztahu je zaměstnanec povinen vykonávat svou práci v rámci stanovené pracovní doby[2] (§2 odst. 2 ZP). Práce musí být odváděna zaměstnancem kvalitně, včasně a osobně (§ 301 písm. b) ZP). Při výkonu práce je zaměstnanec povinen vykonávat svou pracovní činnost nejen v souladu s právními předpisy či pokyny vedoucích zaměstnanců (§301 písm. a) ZP), ale i s dalšími oprávněnými zájmy svého zaměstnavatele (§301 písm. d) ZP).

Zaměstnavatel je pak mj. povinen vytvářet pro výkon práce zaměstnance bezpečné a zdraví neohrožující pracovní prostředí (§ 102 odst. 1 ZP). Dále je mu povinen poskytnout např. potřebné ochranné pracovní prostředky (§104 odst. 1 ZP),

[1] Stanovisko ÚOOÚ č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. Dostupné z: https://www.uoou.cz/files/stanovisko_2009_2.pdf.

[2] § 78 odst. 1 ZP: *„Pracovní dobou rozumíme dobu, v níž je zaměstnanec povinen vykonávat pro zaměstnavatele práci, a dobu, v níž je zaměstnanec na pracovišti připraven k výkonu práce podle pokynů zaměstnavatele.“*

vyžaduje-li to charakter práce. Za zaměstnancem vykonanou práci pak náleží zaměstnanci mzda[3] (§ 109 odst. 1 ZP). V neposlední řadě je zaměstnavatel ve vztahu ke mzdě povinen vydat zaměstnanci v den nástupu do práce písemný mzdový výměr (113 odst. 4 ZP).

K řádnému výkonu sjednaných pracovních povinností mohou být zaměstnancům zaměstnavatelem propůjčovány různorodé výrobní a pracovní prostředky. Dle Morávka přitom není rozhodující, zda se jedná o prostředky, které jsou výlučným vlastnictvím zaměstnavatele, nebo zda se jedná o prostředky pronajaté či půjčené. Podstatné bude vždy pouze to, že se nejedná o prostředky zaměstnance.[4] Mezi prostředky, které jsou poskytovány zaměstnavatelem zaměstnanci, řadíme například mobilní telefony, notebooky, osobní automobily, ale také mobilní data či telefonní tarify. Povinností zaměstnance je svěřené prostředky chránit, a to jak před poškozením či poruchou, tak zneužitím a zcizením (§ 301 písm. d) ZP). Zákoník práce ponechává zcela na zaměstnavateli, zda udělí zaměstnancům souhlas s užíváním svěřených výrobních a pracovních prostředků pro osobní účely. Nejvyšší soud ve svém rozhodnutí ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011 uvádí, že zákaz vyjádřený v ustanovení § 316 odst. 1 ZP je zákazem absolutním. Je proto ponecháno na vůli zaměstnavatele, zda a v jakém rozsahu udělí svým zaměstnancům souhlas k užívání výrobních a pracovních prostředků. Souhlas může být udělen v úplném rozsahu bez omezení. Zaměstnavatel může také svůj souhlas udělit pouze v určitém časovém či věcném rozsahu. Vyloučeno ani není, aby zaměstnavatel uděloval jednorázové souhlasy s užitím výrobních a pracovních prostředků. Například tedy může zaměstnavatel konkrétnímu zaměstnanci umožnit, aby firemní vozidlo využil přes víkend k soukromým účelům.[5]

V případě, že není ze strany zaměstnavatele souhlas s užíváním výrobních a pracovních prostředků zaměstnanci udělen, zaměstnanec nesmí tyto svěřené prostředky užívat k osobním účelům. Zaměstnavatel je oprávněn plnění této povinnosti v souladu s ustanovením § 316 odst. 1 ZP přiměřeným způsobem kontrolovat. Lze oprávněně předpokládat, že zaměstnavatel bude v rámci

[3] § 109 odst. 2 ZP: *„Mzdou rozumíme peněžité plnění a plnění peněžité hodnoty (naturální mzda) poskytované zaměstnavatelem zaměstnanci za práci, není-li v ZP stanoveno jinak.“*
[4] MORÁVEK, J. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy*, 2017, č. 17. s. 573-581.

prováděné kontroly vyhodnocovat, zda jsou v pracovní době svěřené prostředky užívány za účelem výkonu svěřených prací. Shodně tak má zaměstnavatel možnost kontrolovat, zda je pracovní doba využívána zaměstnanci efektivně a k plnění pracovních úkolů. Kromě toho bude zaměstnavatel v rámci kontroly vyhodnocovat, zda není s jeho majetkem nakládáno neoprávněně či způsobem, při kterém dochází k jeho zneužívání. Zaměstnavatel se nemusí omezovat na provedení kontroly pouze v pracovní době. Konkrétním příkladem je situace, kdy došlo ke svěření firemního vozidla zaměstnanci určeného pouze k pracovním účelům. Zde bude GPS lokalizátor ve firemním vozidle zapnutý i mimo pracovní dobu. Morávek k tomuto uvádí, že se dle ust. § 316 odst. 1 ZP postupuje pouze v případě vysoké míry pravděpodobnosti blížící se jistotě, že nemůže být narušeno soukromí zaměstnance. V takovém případě se postupuje bez ohledu na zvolený prostředek kontroly.[6] Typickým příkladem kontroly dle § 316 odst. 1 ZP je nahlížení zaměstnavatele do knihy jízd u propůjčených firemních vozidel. Dalším předpokladem pro provedení kontroly je, že již nedochází ke kontrole dle § 316 odst. 2 ZP.

Zákoník práce u kontroly dle § 316 odst. 1 ZP požaduje, aby byla kontrola prováděná přiměřeným způsobem. Dle Nejvyššího soudu (dále také jako „NS“) představuje § 316 odst. 1 ZP právní normu s relativně neurčitou (abstraktní) hypotézou. Zákoník práce tedy ponechává na jednotlivých soudech, aby samy podle svého pečlivého uvážení v každém jednotlivém případě vymezily hypotézu právní normy ze širokého předem nevymezeného okruhu okolností.[7] Morávek k pojmu *přiměřeným způsobem* uvádí, že pojem *de facto* odkazuje na to, že legálnost kontroly je závislá na zaměstnavatelově záměru. Dále uvádí, že je třeba tento pojem posuzovat ve vztahu ke zvolenému způsobu jeho provedení vzhledem ke všem okolnostem. Jako příklad jednotlivých okolností, které je možno zohlednit, mj. uvádí zvolený způsob a prostředky kontroly, povahu a závažnost kontrolovaných pracovněprávních povinností nebo závažnost chráněných zájmů na straně zaměstnance. Následně bude posuzováno, zda zvolený prostředek k dosažení účelu splňuje podmínku vhodnosti, nutnosti a přiměřenosti s ohledem na zaměstnavatelův záměr a zvolený způsob kontroly.[8]

[6] MORÁVEK, J. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy*, 2017, č. 17. s. 573-581.
[7] Rozsudek Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011.
[8] MORÁVEK, J. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy*, 2017, č. 17. s. 573-581.

V souladu se shora uvedeným rozhodnutím NS je dle mého názoru potřebné, aby byly výše uvedené neurčité právní pojmy interpretovány v kontextu konkrétně prováděné kontroly, jakož i osoby zaměstnance a zaměstnavatele. Shodně by tak dle mého názoru měla být kontrola prováděna pouze v nezbytném rozsahu. Při své úvaze totiž vycházím především z toho, že právo zaměstnance na soukromý život by pro zaměstnavatele mělo být vždy prioritou.

Ustanovení § 316 odst. 2 ZP se vztahuje ke kontrolním mechanismům zaměstnavatele spočívajících v otevřeném nebo skrytém sledování zaměstnance, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontroly listovních zásilek adresovaných zaměstnanci (§ 316 odst. 2 ZP). Výčet kontrolních mechanismů v tomto ustanovení je pouze výčtem demonstrativním. Důvodem je rozvoj a modernizace technologií. Z praxe a rozhodovací činnosti soudů v České republice i soudů členských států EU můžeme vypozorovat nové kontrolní mechanismy, které lze podřadit pod monitoring. Jako příklad lze uvést jednání společnosti IKEA Ltd. Ve Francii Společnost IKEA Ltd. najímala falešné pracovníky za účelem sledování svých zaměstnanců a získávání informací nejen o jejich pracovní výkonnosti.[9] Jednotlivým formám monitoringu bude v rámci diplomové práce věnována pozornost v druhé kapitole.

Odstavec třetí § 316 ZP ukládá zaměstnavateli povinnost informovat své zaměstnance o rozsahu a způsobu kontroly dle ust. § 316 odst. 2 ZP. Ustanovení § 316 odst. 2 a odst. 3 ZP stanovují podmínky, za kterých může zaměstnavatel zasáhnout do práva na soukromí zaměstnance. Právo na soukromí je v obecné rovině garantováno v Listině základních práv a svobod[10] (dále také jako „Listina“). Podmínky, které musí zaměstnavatel při monitoringu zaměstnanců splnit, jsou následující:

- Zaměstnavatel musí mít pro kontrolu závažný důvod.
- Závažný důvod musí spočívat ve zvláštní povaze činnosti zaměstnavatele.
- Zaměstnavatel musí své zaměstnance seznámit s těmito kontrolními mechanismy. Zaměstnanci musí být především srozuměni s rozsahem realizované kontrolní činnosti. Dále pak se způsobem, jakým má být kontrola prováděna.

[9] BBC. *Ikea France fined €1m for snooping on staff*. [online]. Publikováno 15. 6. 2021 [cit. 31. 3. 2022]. Dostupné z: https://www.bbc.com/news/world-europe-57482168.
[10] Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.

Osobně za velmi problematické vnímám to, že se v rámci shora uvedeného ustanovení vyskytují neurčité právní pojmy, a to *závažný důvod* a *zvláštní povaha činnosti zaměstnavatele.* Zda byla v konkrétním případě splněna podmínka závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele, je nutné posuzovat ve vztahu ke konkrétní prováděné kontrole. Důraz je kladen na princip proporcionality. Dle tohoto principu je posuzováno, zda provedený kontrolní mechanismus umožňuje zaměstnavateli dosáhnout jím stanoveného cíle. Dále je posuzováno, zda by nemohlo být cíle dosaženo užitím jiných, méně invazivních kontrolních mechanismů. V neposlední řadě je velice důležité také zohlednit, bude-li v konkrétní situaci převažovat zájem na ochranu vlastnického práva zaměstnavatele, nebo zaměstnancovo právo na soukromí.

V zájmu ochrany svých majetkových práv je zaměstnavatel dále oprávněn v nezbytném rozsahu kontrolovat, jaké věci zaměstnanci vynášejí a vnášejí na a z pracoviště. V souvislosti s tím je zaměstnavatel oprávněn provádět prohlídky zaměstnanců. Zaměstnavatel však musí dbát na dodržování ochrany osobnosti (§ 248 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů dále také jako „občanský zákoník“ nebo „ObčZ“).

Kontrola nemusí být prováděna přímo zaměstnavatelem, ale může být svěřena např. bezpečností agentuře, která dozoruje u tzv. turniketů[11]. Velmi často jsou turnikety u výrobních společností, kde zaměstnanci mohou snadno pronést např. měděné dráty. Má-li být přistoupeno k provedení osobní prohlídky zaměstnance, je nutné, aby byla tato prohlídka provedena osobou stejného pohlaví.

Osobně se domnívám, že lze tyto kontroly oprávněně očekávat především u výrobních společností, ve kterých je pracováno s drahým materiálem, například s platinou, mědí, zlatem či hliníkem. Účelné mohou být dále kupř. u prodavačů v obchodních centrech (např. u prodejců elektroniky), kde reálně může docházet ke vzniku nezanedbatelných škod na majetku zaměstnavatele.

1. 2 Listina základních práv a svobod

Jak vyplývá z předchozí podkapitoly, při monitorování zaměstnanců je zaměstnavatelem velmi často zasahováno do soukromí zaměstnance. Právo na ochranu soukromého života je právem, které je každému z nás garantováno Listinou. Významnost zachování práva na soukromý život lze dovodit

[11] Turniketem rozumíme zařízení fungující jako brána, kterou může projít v daný okamžik pouze jeden člověk.

i z mezinárodních smluv, kterými je Česká republika v souladu se čl. 10 Ústavy vázána.[12]

Vymezení pojmů *soukromí* a *soukromý život* z hlediska práva je velmi složité a domnívám se, že téměř nemožné. Waren a Brandeis kupříkladu nahlíží na právo na soukromí jako na právo být ponechán o samotě.[13] ÚOUU pak stručně popsal *soukromí* jako: *„osobní, intimní sféru člověka v jeho integritě, která zahrnuje všechny projevy osobnosti konkrétního a jedinečného lidského tvora. Pojem soukromí obsahuje rovněž hmotný i myšlenkový prostor jednotlivce, součástí soukromého života je i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.“*[14]

Výkladem pojmu *soukromý život zaměstnanců* se v rámci své rozhodovací praxe opakovaně zabýval Evropský soud pro lidská práva (dále také jako „ESLP“). Dle judikatury ESLP je pod pojmem *soukromí* nutno rozumět právo každého člověka na to, aby vytvářel a rozvíjel vztahy s ostatními lidmi. Tyto vztahy každý jednotlivec rozvíjí jak v kruhu rodinném, tak na pracovišti. Do rodinného kruhu řadíme především vztahy mezi rodinnými příslušníky či blízkými přáteli. Vztahy na pracovišti jsou rozvíjeny jak mezi podřízenými, nadřízenými, tak spolupracovníky. Vztahy na pracovišti tvoří důležitou součást osobních mezilidských interakcí. Hlavním důvodem je množství času, který každý z nás tráví na svém pracovišti. Z daného důvodu není možné najít striktní hranici mezi životem ryze soukromým a tím pracovním. Z tohoto důvodu je nutné pod pojem *právo na respektování soukromého života* subsumovat též právo na soukromí na pracovišti.[15]

Nelze po zaměstnanci spravedlivě požadovat, aby na pracovišti nenavazoval vztahy se svými kolegy. Shodně tak nelze spravedlivě požadovat, aby každou vteřinu na pracovišti věnoval ryze pracovním záležitostem. Představíme-li si například situaci, kdy matce samoživitelce zavolá učitelka ze školky, že je její dítě nemocné, bude nutné, aby si telefonát v práci vyřešila. Na druhou stranu je však nutné uvést i to, že zaměstnavatel je zajisté oprávněn po zaměstnanci požadovat, aby tyto soukromé záležitosti v pracovní době a na pracovišti vyřizoval pouze

[12] Sdělení č. 209/1992 Sb., Sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.
[13] WARREN, S. D., BRANEIS, L. D. The Right to Privacy *The Harward Law Review*. [online]. 1890, roč. 4, č. [cit. 31. 3. 2022]. Dostupné z: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.
[14] Stanovisko ÚOOÚ č. 6/2009: Ochrana soukromí při zpracování osobních údajů. Listopad 2009, aktualizace. Dostupné z: https://www.uoou.cz/files/stanovisko_2009_6.pdf.
[15] Rozsudek ESLP ze dne 16. prosince 1992, Niemitz versus Německo, č. stížnosti 13710/88.

v nezbytném a v přiměřeném rozsahu. Lze oprávněně očekávat, že zaměstnavatel nebude souhlasit s tím, aby výše zmíněná matka samoživitelka telefonovala po většinu své pracovní doby s kamarádkou, např. za účelem výběru letní dovolené.

Domnívám se, že každý z nás očekává určitou míru soukromí na pracovišti. Například předpokládáme, že nám jak zaměstnavatel, tak spolupracovníci nebudou nahlížet do jednotlivých šuplíků u pracovních stolů. Jsme přesvědčeni, že zaměstnavatel nebude sledovat toalety, šatny a další místnosti, ve kterých by mohl zasáhnout naší intimní sféru.[16] Zde lze poukázat na rozhodnutí ESLP ze dne 26. července 2007, stížnost č. 64209/01 Peev proti Bulharsku. Po rezignaci pana Peeva, který působil jako expert u Rady pro kriminologická studia při Nejvyšším kasačním zastupitelství, byla jeho zaměstnavatelem provedena kontrola jeho kanceláře. Zaměstnavatel vypracoval velmi podrobný soupis věcí, které byly nalezeny v zásuvkách a kartotékách psacího stolu v kanceláři pana Peeva. Tento soupis obsahoval mj. kompaktní disky s jeho osobními záležitostmi, lékařské zprávy a osobní fotografie. Zaměstnavatel dále provedl kontrolu pevného disku pana Peeva a sepsal soupis zjištění. ESLP se zabýval tím, zda představoval přístup zaměstnavatele do pracovního stolu zaměstnance porušení práva na jeho soukromí garantovaného ve čl. 8 Sdělení č. 209/1992 Sb., Sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících (dále také jako „Úmluva“). ESLP dospěl k názoru, že ano. Peev měl v daném případě přiměřené očekávání soukromí. To mj. podpořila i skutečnost, že měl Peev v zásuvkách stolu osobní dokumenty, např. fotografie apod. ESLP se dále vyjádřil k pojmu *soukromý život*. ESLP uvedl, že se pojem *soukromý život* jasně vztahuje kromě jiného také na telefonní hovory z firemních prostor a na e-maily, které jsou odesílány z práce.[17]

Ochranu před neoprávněným zásahem do rodinného a soukromého života poskytuje jednotlivci čl. 10 Listiny. Dále zde nacházíme také právo na ochranu před zneužíváním a neoprávněným shromažďováním osobních údajů. Čl. 10 Listiny však nelze vnímat jako jediný, který v sobě zakotvuje ochranu soukromé sféry jednotlivce. Dalším důležitým ustanovením je také čl. 13 Listiny. Tento článek pojednává o ochraně listovního tajemství a tajemství dalších písemností a záznamů.

[16] Úřad pro ochranu osobních údajů. *K provozování kamerových systémů*. Nejčastější otázky a odpovědi. [online]. © 2013 [cit. 31. 3. 2022]. Dostupné z: https://www.uoou.cz/k-provozovani-kamerovych-systemu/d-29535.
[17] Rozsudek ESLP Coplandová versus Spojené království ze dne 3. dubna 2007, č. stížnosti 62617/00.

V této souvislosti bych ráda zmínila usnesení Ústavního soudu ze dne 31. března 2009, sp. zn. I. ÚS 452/09. Ústavní soud v tomto usnesení řešil případ, kdy zaměstnanec užil pro soukromé záležitosti pracovní notebook určený k plnění pracovních úkolů. Současně proběhlo řádné poučení zaměstnance o tom, že zaměstnavatel provádí monitoring připojení na internet a zajišťuje výpisy z připojení. Z těchto výpisů bylo možné zjistit, jaký konkrétní uživatel webové stránky navštívil. Zaměstnanec i přes to navštívil na internetu webové stránky za účelem soukromých záležitostí. Následně zaměstnavatel policejnímu orgánu[18] předložil detailní výpis připojení. Ústavní soud shledal toto jednání v souladu s čl. 13 LZPS a uvedl, že nebylo zasaženo do práva na soukromí zaměstnance.

Osobně s Ústavním soudem souhlasím a domnívám se, že ve výše uvedené situaci zaměstnanec nemůže legitimně očekávat soukromí. Zaměstnanec byl předem zaměstnavatelem srozuměn s tím, že jeho připojení na internet je monitorováno. Zaměstnanec tedy stránky musel navštěvovat již s vědomím, že se o jeho aktivitě může zcela oprávněně dozvědět zaměstnavatel.

Jak bylo výše uvedeno, zaměstnanci mají legitimní očekávání soukromí na pracovišti. Jak uvádí Pracovní skupina[19], toto právo musí být v rovnováze s ostatními oprávněnými právy a zájmy zaměstnavatele. Zejména musí být v souladu s právem zaměstnavatele v určitém rozsahu účelně provozovat svou podnikatelskou činnost. Konkrétně hovoříme o právu zaměstnavatele chránit se před odpovědností nebo újmou[20]. Shodně bude proti právu zaměstnance na ochranu rodinného a soukromého života stát ochrana vlastnického práva zaměstnavatele. Ochranu vlastnického práva garantuje čl. 11 Listiny. Toto ustanovení konkrétně chrání jak svěřené prostředky jako např. firemní automobily, notebooky aj., tak např. o ochranu *know how* či firemních systémů.

1. 3 Občanský zákoník

Nejvyšší soud ve svém rozsudku ze dne 26. 7. 2000, sp. zn. 30 Cdo 2304/99 uvedl k pojmu *osobnost člověka*, že představuje „*nejvlastnější, nejniternější a*

[18] Vůči zaměstnankyni bylo totiž zahájeno trestní stíhání pro podezření ze spáchání trestného činu poškozování cizích práv. Zaměstnankyně z firemního počítače sdílela polonahé fotografie třetí osoby na veřejně přístupných webových stránkách. Proto byl zaměstnavatel policejním orgánem vyzván k poskytnutí výpisu internetového připojení.

[19] Pracovní skupina byla nezávislým evropským poradním orgánem na ochranu dat a soukromí. Ustanovena byla článkem 29. směrnice 95/46/EC. Účinností GDPR pracovní skupinu nahradil Evropský sbor pro ochranu osobních údajů.

[20] Pracovní dokument WP29: Ke sledování elektronických komunikací na pracovišti (v originále: *Working document on the surveillance of electronic communications in the workplace*).

nejintimnější sféru lidské osoby, jejíž dotčení zvenčí je zásahem dotčenou fyzickou osobou velmi často pociťováno se značně nepříznivou intenzitou". Je proto nezbytné, aby byla této sféře každého z nás poskytována dostatečná právní ochrana.

Právní ochrana osobnosti člověka je vymezena v části první, hlavě druhé, oddílu šestém občanského zákoníku. V této části jsou obsažena ustanovení, která upravují ochranu osobnosti člověka. Tůma k osobnosti člověka uvádí, že občanský zákoník upravuje pouze takové stránky lidské osobnosti, které lze nalézt u každého člověka.[21] Hovoříme tedy o osobnostních právech, které náleží každé fyzické osobě. Tato práva se tedy nevztahují ke zvláštním projevům osobnosti souvisejících výlučně s uměleckou, technickou či vědeckou tvorbou.[22]

Za generální klauzuli ochrany osobnosti lze označit § 81 odst. 1 ObčZ. Podle tohoto ustanovení je nutno chránit osobnost člověka spolu se všemi jeho nezadatelnými, vrozenými, přirozenými právy. Dále je nutno ctít jeho rozhodování o tom, jak chce žít (§ 81 odst. 1 ObčZ). V případě zásahu do osobnosti člověka má každý, kdo je tímto zásahem dotčen právo domáhat se toho, aby bylo od tohoto zásahu upuštěno a následku odstraněno (§ 81 odst. 2 ObčZ). Jedním z nástrojů, který může být zaměstnancem k ochraně jeho osobnosti využit, je žaloba v civilním soudnictví. Případně může zaměstnanec zvolit postup, v němž bude jednat prostřednictvím podnětu k inspektorátu práce či ÚOOÚ.

V § 86 ObčZ je zakotveno právo na soukromí. Obdobně jako zákoník práce požaduje i občanský zákoník pro zásah do soukromí jednotlivce legitimní důvod. Má-li být sledován soukromý život jednotlivce, je vyžadováno udělení souhlasu sledovaného. Ve stejném rozsahu občanský zákoník chrání i soukromé písemnosti osobní povahy (§ 86 ObčZ).

1. 4 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném

[21] TŮMA, P. In: LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. 2. vydání. Praha: C. H. Beck, 2022. marg. č. 36. s. 2380. § 81 [Osobnost člověka].
[22] Ochrana zvláštních projevů osobnosti je svěřena zvláštním právním předpisům upravujícím např. ochranu duševního vlastnictví.

pohybu těchto údajů (dále také jako „GDPR“)[23] navazuje na úpravu obsaženou ve směrnici 95/46/ES[24]. Příčin, pro které došlo k vydání GDPR, lze shledat několik. Hlavním důvodem byla síla původního dokumentu, který byl vydán ve formě směrnice. Ta na rozdíl od nařízení stanovuje pouze cíl, kterého musí jednotlivé členské EU dosáhnout. Směrnice však přesně nekonkretizuje, jakým způsobem a prostředky má být tohoto cíle dosaženo. Dalším důvodem je, že právní úprava ochrany a zpracovávání osobních údajů napříč EU byla v době přijímání GDPR roztříštěná. V souvislosti s touto roztříštěností docházelo k vytváření bariér v oblasti volného pohybu osobních údajů. Stejně tak i směrnice 95/46/ES byla vydávána v době, kdy přístup k internetu nebyl natolik jednoduchý a dostupný, jako je dnes. Hovoříme o době, kdy IT technologie byly na počátku svého rozkvětu.[25] Bylo proto nutné na roztříštěnost a technologický pokrok zareagovat. Řešením bylo právě sjednocení a zpřesnění právních úprav zpracovávání osobních údajů napříč členskými státy EU.

GDPR je univerzálním právním předpisem s přímou použitelností pro všechny členské státy EU. Ve vztahu k monitorování zaměstnanců je podstatné zmínit především čl. 88 GDPR, dle kterého: *„Členské státy mohou právním předpisem nebo kolektivními smlouvami stanovit konkrétnější pravidla k zajištění ochrany práva a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním.“* Tento článek svěřuje členským státům EU pravomoc konkretizovat pravidla k zajištění řádného zpracování osobních údajů zaměstnanců.

Myslím si, že zakotvení tohoto článku do GDPR je logickým krokem. Evropská unie je tvořena 27 členskými státy, jejichž právní řády jsou postaveny na jiných hodnotách a tradicích. V těchto státech je odchylná i právní úprava pracovního práva. Právě z tohoto důvodu kvituji, že nebyla striktně stanovena jednotná právní úprava pro všechny členské státy. Neznamená to však, že by si členské státy mohly upravovat pravidla svévolně. Z článku 88 GDPR vyplývají následující omezení:

[23] Nařízení je dle čl. 288 SFEU charakteristické svou obecnou působností, závazností v plném rozsahu a přímou použitelností ve všech členských státech.
[24] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
[25] Přehledně: Novinky.cz. *Jak se měnil internet v Česku*. [online]. Publikováno 14. 2. 2017. [cit. 31. 3. 2022]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/prehledne-jak-se-menil-internet-v-cesku-40024418.

- ke konkretizaci musí dojít na základě právního předpisu, případně kolektivními smlouvami,
- úprava musí být přijata za účelem zajištění ochrany práv a svobod,
- zajištění práv a svobod musí být provedeno ve vztahu ke zpracování osobních údajů, a to v souvislosti se zaměstnáním.

Mezi účely, pro které mohou být stanovena konkrétní pravidla GDPR, jsou jmenovány např. plnění pracovní smlouvy, organizace práce či ochrana majetku zaměstnavatele. Právě poslední z výše zmiňovaných účelů je klíčovým pro problematiku monitoringu zaměstnanců. Zemanová Šimonová v souvislosti s úpravou čl. 88 GDPR uvádí, že právní normy přijímané jednotlivými členskými státy musí obsahovat opatření zajišťující ochranu lidské důstojnosti nebo oprávněných zájmů.[26] Obsažena by ale měla být též vhodná opatření, která budou zajišťovat ochranu základních práv zaměstnanců. Tato opatření by měla být zahrnuta mj. tehdy, pokud se jedná o systém monitorování na pracovišti (čl. 88 odst. 2 GDPR). Rámiš se domnívá, že ačkoliv čl. 88 odst. 2 GDPR primárně směřuje na ochranu práv a svobod zaměstnanců, neměly by být při přijímání vnitrostátní právní úpravy opomíjeny ani základní práva zaměstnavatelů. Tvrdí, že dokonce není ani vyloučeno, aby zákonodárce v České republice omezil jednotlivá práva zaměstnanců za účelem ochrany třetích osob (zpravidla zaměstnavatelů).[27]

Z vnitrostátních právních předpisů, které konkretizují pravidla k zajištění práv a svobod ve vztahu ke zpracovávání osobních údajů lze uvést jako stěžejní následující právní předpisy:

- zákon č. 110/2019 Sb., zákon o zpracování osobních údajů,
- zákon č. 262/2006 Sb., zákoník práce,
- zákon č. 435/2004 Sb., zákon o zaměstnanosti.

Dle Zemanové Šimonové je nutné na vztah mezi GDPR a přijatou či existující vnitrostátní právní úpravou nahlížet jako na vztah obecného a speciálního právního předpisu.[28] Tento vztah vychází z obecného právního *principu lex specialis derogat legi generali*. Primárně je aplikována vnitrostátní právní úprava.

[26] ZEMANOVÁ ŠIMONOVÁ, H. Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů. *Bulletin advokacie*. 2017, č. 9. s. 25-32. ISSN 1210-6348.
[27] RÁMIŠ, V. In: UŘIČAŘ, M., RÁMIŠ, V. a kol. *Obecné nařízení o ochraně osobních údajů.* 1. vydání. Praha: C. H. Beck, 2021, s. 1283, marg. č. 23. Článek 88 [Zpracování v souvislosti se zaměstnáním].
[28] ZEMANOVÁ ŠIMONOVÁ, H. Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů. *Bulletin advokacie*. 2017, č. 9. s. 25-32. ISSN 1210-6348.

Zaměstnavatele lze v souladu s GDPR označit za správce údajů, zaměstnance pak za subjekt údajů. GDPR vytyčuje zásady, které musí být správcem údajů, tj. zaměstnavatelem, při zpracování osobních údajů, dodrženy. Dle GDPR musí zaměstnavatel zpracovávat osobní údaje ze zákonem stanovených důvodů, a to korektně a transparentně. S odkazem na požadavek transparentnosti má být zaměstnavatel schopen zaměstnanci konkretizovat, na základě jaké právní normy jsou jeho údaje zpracovávány. Stejně tak má být zaměstnavatel schopen poskytnout zaměstnanci informace o tom, za jakým konkrétním účelem, v jakém rozsahu a v neposlední řadě, jakými prostředky ke zpracování údajů dochází. Tyto informace by měl zaměstnavatel podávat zaměstnanci jednoduchým způsobem tak, aby byly ze strany zaměstnance jednoduše pochopitelné. Informační povinnost blíže rozvádí čl. 13 a čl. 14 GDPR. Zásah zaměstnavatele musí vždy být prováděn v nezbytném rozsahu a k účelu, pro který je činěn (čl. 5 GDPR). Zpracovávání osobních údajů musí sledovat legitimní účel, který musí být zaměstnavatel schopen řádně odůvodnit. Pod legitimním účelem si lze představit například oprávněný zájem zaměstnavatele na ochraně jeho majetku či zajištění bezpečnosti na pracovišti zaměstnavatele. Šmíd pak pod legitimní účel podřazuje např. ochranu duševního vlastnictví společnosti nebo monitoring pro účely zvýšení produktivity zaměstnanců.[29]

I GDPR svěřuje subjektu údajů, tj. i zaměstnancům, prostředky právní ochrany, které lze v rámci pracovněprávního vztahu využít. Bude-li mít zaměstnanec za to, že zaměstnavatel zpracoval jeho údaje v rozporu s GDPR, je oprávněn podat stížnost u dozorového úřadu. Tímto dozorovým úřadem je v ČR Úřad pro ochranu osobních údajů.[30]

Místní příslušnost dozorového úřadu je nařízením určena dle obvyklého bydliště, místa výkonu zaměstnání nebo také místem, kde došlo k porušení GDPR (čl. 77 GDPR). Uplatněním stížnosti není dotčeno právo zaměstnance na uplatnění jiných prostředků správní či soudní ochrany. GDPR stanovuje dozorovému úřadu povinnost vyrozumět subjekt údajů o výsledku řízení o jím podané stížnosti (čl. 77 GDPR).

---

[29] ŠMÍD, V. In.: ePrávo.cz. *Zpracování osobních údajů zaměstnanců s přihlédnutím k možnosti sledování produktivity*. [online]. Publikováno 27. 8. 2018. [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/zpracovani-osobnich-udaju-zamestnancu-s-prihlednutim-k-moznosti-sledovani-produktivity-108065.html.

[30] Působnost a postavení tohoto úřadu dále rozvádí zákon č. 110/2019 Sb., o zpracování osobních údajů.

Dozorový úřad je dle GDPR nečinný v případě, kdy nevyrozumí subjekt údajů o průběhu řízení nejpozději do tří měsíců od přijetí stížnosti, nebo pokud se přijatou stížností nezačne vůbec zabývat. V případě nečinnosti dozorového úřadu pak subjekt údajů může využít institut žaloby proti nečinnosti, jež je upravena v zákoně č. 150/2002 Sb., soudní řad správní.

1. 5 Zákon o zpracování osobních údajů

Zákon č. 110/2019 Sb., o zpracování osobních údajů (dále také jako „zákon o zpracování osobních údajů“) implementoval do právního řádu České republiky GDPR a Směrnici 2016/680[31]. V rámci české právní úpravy navázal na původní právní úpravu problematiky zpracování osobních údajů, která byla obsažena v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Ústřední institucí v souvislosti s touto problematikou je Úřad pro ochranu osobních údajů. Jedná se o dozorový orgán ve smyslu GDPR a ústřední správní úřad v oblasti ochrany a zpracování osobních údajů. Jeho postavení a pravomoci blíže upravuje hlava V. zákona o zpracování osobních údajů.

ÚOOÚ je pověřen kontrolou aplikování GDPR. Do jeho působnosti tak mj. spadá poskytování ochrany v oblasti ochrany a zpracovávání osobních údajů, kontrola implementace GDPR a jeho dodržování ze strany správců a zpracovatelů[32]. Zákon o zpracování osobních údajů dále stanovuje, že ÚOOÚ: „*zvyšuje povědomí veřejnosti o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním a podporuje porozumění těmto otázkám“* (čl. 57 odst. 1. písm. b) GDPR).

Mezi nástroje ÚOOÚ, kterými se ÚOOÚ snaží o navýšení povědomí společnosti o problematice ochrany a zpracovávání osobních údajů lze zařadit jím vydávané právní akty. Jedná se především o stanoviska a rozhodnutí. Ty jsou volně k dispozici na webových stránkách ÚOOU.[33] V souvislosti s monitoringem zaměstnanců lze označit za významná především následující stanoviska:

- **Stanovisko ÚOOÚ č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů**. Za jeho přínos pro

[31] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

[32] Zpracovatelem osobních údajů je ten, kdo jménem správce údajů zpracovává osobní údaje. Pro zaměstnavatele často zpracovávají osobní údaje např. externí poskytovatelé pracovnělékařských či mzdových služeb.

[33] Např. Úřad pro ochranu osobních údajů. *Rozhodnutí předsedy úřadu*. [online]. © 2013[cit. 31. 3. 2022]. Dostupné z: https://www.uoou.cz/rozhodnuti-predsedy-uradu/ds-3815.

problematiku monitoringu lze dle mého názoru označit především to, že stanovuje povinnosti správce (v našem případě zaměstnavatele) při provozování kamerového systému.

- **Stanovisko ÚOOÚ č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště**. Za jeho přínos pro problematiku monitoringu lze dle mého názoru označit naopak to, že blíže stanovuje a rozvádí klíčové zásady, se kterými musí především zaměstnavatel v rámci monitoringu kooperovat. Těmito zásadami jsou: zásada proporcionality, zásada přiměřenosti, zásada analogie a informační povinnost. Bližší pozornost bude některým z těchto zásad a věnována ve třetí kapitole.
- **Stanovisko ÚOOÚ č. 6/2012: Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů**. Zde je v prvé řadě nutno uvést, že toto stanovisko odkazuje na dřívější právní úpravu, a to tu, která byla obsažena v zákoně o ochraně osobních údajů. Současná právní úprava však oznamovací povinnost nevyloučila. I toto stanovisko nám tak může posloužit jako pomocné vodítko při interpretaci a pochopení problematiky monitoringu zaměstnanců.

1. 6 Zákon o inspekci práce

Zákon č. 251/2005 Sb., o inspekci práce (dále také jako „zákon o inspekci práce“ nebo „ZoIP“) zakotvuje postavení orgánů inspekce práce a jejich postup při dozoru nad dodržováním pracovněprávních předpisů. Zákon o inspekci práce dále vymezuje skutkové podstaty správních deliktů a sankce, které lze za jejich spáchání uložit. K porušení pracovněprávních předpisů může zaměstnavatelem dojít i při monitorování zaměstnanců. Skutkové podstaty přestupků v segmentu ochrany soukromí a osobních práv zaměstnanců vymezuje § 11a odst. 1 písm. a) až c) ZoIP[34]. Skutkové podstaty správních deliktů se vztahují k porušení ust. § 316 ZP. Zaměstnavatel může být sankcionován kromě nesplnění informační povinnosti dle § 316 odst. 3 ZP (§11a odst. 1 písm. b) ZoIP)[35], také za narušení a zásah do soukromí zaměstnance na pracovišti či ve společných prostorech zaměstnavatele,

[34] Je-li zaměstnavatel právnickou osobou, jsou skutkové podstaty přestupků v segmentu ochrany soukromí a osobnostních práv zaměstnanců vymezeny v ust. § 24a odst. 1 písm. a) až c) ZoIP.
[35] U zaměstnavatele, který je právnickou osobou viz. § 24a odst. 1 písm. b) ZoIP.

některým ze způsobů dle ust. § 316 odst. 2 ZP (§ 11a odst. 1 písm. a) ZoIP[36]). Každý zaměstnanec, který se cítí na svých právech zkrácen monitorováním ze strany zaměstnavatele, je oprávněn obrátit se se svým podnětem k provedení kontroly. Vyjma ÚOOÚ realizuje kontrolní činnost v oblasti ochrany a zpracování osobních údajů i další ze správních úřadů. Těmito úřady jsou Státní úřad inspekce práce a jemu podřízené oblastní inspektoráty práce. Jejich působnost a pravomoc je blíže vymezena v zákoně č. 251/2005 Sb., o inspekci práce.

Podnět k provedení kontroly může být podán písemně, osobně či elektronicky (např. e-mailem, datovou schránkou). Podnět je dále možné podat prostřednictvím elektronického formuláře.[37] Dle mého názoru lze vnímat elektronický formulář za pozitivní institut. Jedním z důvodů je fakt, že v dnešní technologicky nadané době má přístup k internetu téměř každý. Oproti osobně podanému podnětu lze pozitivně kvitovat i zvýšenou anonymizaci. Výhody elektronického formuláře mj. bylo možné pozorovat době, kdy byly v souvislosti s pandemií onemocnění covid-19 na mnohých úřadech omezovány úřední hodiny. Díky elektronickým formulářům mohlo dojít k nižšímu kontaktu mezi zaměstnanci úřadů a veřejností. Elektronický formulář je navíc možné odeslat kdykoliv, tedy i mimo úřední hodiny, což je jeho nespornou výhodou. Na základě přijatého podnětu může být zahájena kontrola za účelem ověření plnění pracovněprávních předpisů. Na kontrolní činnost bude subsidiárně aplikován zákon č. 255/2012 Sb., o kontrole.

1. 7 Trestní zákoník

Pro úplnost je nutné zmínit též zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů (dále také jako „TZ“). Mezi klasické formy monitoringu patří monitoring e-mailů či mobilních telefonů. Zaměstnavatel by u těchto forem monitoringu měl postupovat tak, aby minimalizoval možnost seznámit se s obsahem e-mailových či SMS zpráv. Důvod, pro který by zaměstnavatelé měli při monitoringu počínat obezřetně spočívá v tom, že tyto zprávy požívají zákonné ochrany. Právo zaměstnance na zachování soukromí a respektu k jeho korespondenci je zakotveno ve čl. 13 Listiny a čl. 8 Úmluvy. Pokud zaměstnavatel úmyslně otevře e-mail zaměstnance ryze osobního charakteru a poruší tím tajemství takto zaslané zprávy, dopustí se v souladu s ust. § 182 odst.

[36] U zaměstnavatele, který je právnickou osobou viz. § 24a odst. 1 písm. a) ZoIP.
[37] Státní úřad inspekce práce. *Podání podnětu*. [online]. Publikováno © 2022. [cit. 31. 3. 2022]. Dostupné z: http://epp.suip.cz/epp/index_light.php.

1 písm. b) TZ trestného činu *porušení dopravovaných zpráv.* Takového trestného činu se může dopustit i zaměstnavatel, který je právnickou osobou.[38] Šámal ve své učebnici zdůrazňuje, že ust. §182 odst. 2 TZ poskytuje ochranu obsahu doručených zpráv bez ohledu na to, jakou osobní hodnotu mají tyto zprávy pro adresáta či odesílatele. Dle Šámala se pak ochrana týká i zpráv profesní povahy, například pozvánek na firemní akce. K naplnění skutkové podstaty trestného činu dopravovaných zpráv postačí pouhé otevření e-mailové či SMS zprávy.[39]

V odborných článcích se můžeme setkat i s odkazem na § 180 TZ, který upravuje skutkovou podstatu trestného činu *neoprávněné nakládání s osobními údaji*. Zde si dovolím upozornit, že § 180 odst. 1 TZ se vztahuje na neoprávněné nakládání s osobními údaji, které byly shromážděny v souvislosti s výkonem veřejné moci. Orgánem veřejné moci rozumíme například soudy, zdravotní pojišťovny či jednotlivá ministerstva. Toto ustanovení tedy nelze interpretovat ve vztahu ke všem osobním údajům. Osobním údajem shromážděným v souvislosti s výkonem veřejné moci může být například údaj sdělovaný daňovým orgánům, tj. například daňové přiznání. Za situace, kdy zaměstnavatel bude neoprávněně sdílet daňová přiznání svých zaměstnanců, by tedy zaměstnavatel mohl naplnit charakteristiky i této skutkové podstaty. Předpokládám však, že se s takovými trestnými činy i s trestnými činy dle odst. 2 tohoto ustanovení budeme setkávat pouze výjimečně.

1. 8 Evropská úmluva o ochraně lidských práv a základních svobod

Evropská úmluva o ochraně lidských práv a základních svobod byla uzavřena v roce 1950. Jedná se o dokument Rady Evropy, který navazuje na Všeobecnou deklaraci lidských práv[40]. Rada Evropy přijímala Úmluvu s cílem dosáhnout jednoty mezi členskými státy, ochrany a rozvoje lidských práv a základních svobod.

Pro téma diplomové práce je stěžejní především čl. 8 Úmluvy. Ten zakotvuje právo na respektování soukromého a rodinného života. Dle tohoto článku má každý právo na respektování soukromého a rodinného života, obydlí

38 Srov. §7 zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, v pozdějším znění.
39 ŠÁMAL, P. In.: ŠÁMAL, P., NOVOTNÝ, O., GŘIVNA, T. a kol. *Trestní právo hmotné.* 8. přepracované vydání. Praha: Wolters Kluwer, s. 613. 2016. ISBN 978-80-7552-358-7.
40 Všeobecná deklarace lidských práv byla vyhlášena 10. prosince 1948 Valným shromážděním Organizace spojených národů.

a korespondence. Odstavec druhý pak zakazuje státním orgánům zasahovat do práva na respektování soukromého a rodinného života a dále stanovuje výjimky, za kterých k takovému zásahu může státní orgán přistoupit.

Jak bylo uvedeno v kapitole *1. 2 Listina základních práv a svobod* této diplomové práce, právo na soukromí má zaměstnanec i na svém pracovišti. Ve čl. 8 Úmluvy však definici soukromí nenacházíme. Dle mého názoru se proto i zde ponechává na soudu, aby v konkrétním případě rozhodl o tom, zda došlo k porušení práva na soukromí či nikoliv. To mj. Evropský soud pro lidská práva pravidelně činí.

ESLP zde vychází z tzv. testu rozumného očekávání soukromí (*reasonable expectation of privacy*), někdy též jako test legitimního očekávání (l*egitimate expectation*)[41]. Byť nikde konkrétně na tento test neodkazuje, uplatňuje jej pravidelně. Vnímám proto za podstatné ho v této kapitole uvést. Dle Fialové je u testu legitimního očekávání nutno vycházet ze dvou kritérií. První, subjektivní kritérium, vyjadřuje aktuální očekávání práva na soukromí v konkrétní situaci. Druhé, objektivní kritérium, spočívá v tom, zda společnost toto očekávání označuje za přiměřené.[42]

Při testu, zda došlo k porušení čl. 8 Úmluvy si ESLP při svém rozhodování klade následující otázky:

- Bylo porušeno právo na respektování soukromého a rodinného života dle čl. 8 Úmluvy?
- Bylo právo omezeno?
- Bylo-li právo omezeno, bylo omezeno v souladu se čl. 8 odst. 2 Úmluvy?
- Bylo takové omezení práva na respektování soukromého a rodinného života dle čl. 8 Úmluvy nezbytné? Neexistovaly jiné, mírnější prostředky?

1. 9 Ostatní prameny

V souvislosti se vstupem České republiky do EU nelze opomíjet ani nezávazné dokumenty, které jsou vydávány jednotlivými poradními institucemi orgánů EU. Tyto dokumenty sice nelze formálně řadit mezi právní předpisy, ale

[41] Srovnej. Rozhodnutí Evropského soudu pro lidská práva, stížnost č. 63737/00, §§36-43, Perry proti Spojenému království, nebo rozhodnutí Evropského soudu pro lidská práva, stížnost č. 44787/98, §57 PG a JH proti Spojenému království.

[42] FIALOVÁ, E. Ochrana soukromí ve světle judikatury Evropského soudu pro lidská práva. *Časopis pro právní vědu a praxi.* [online]. Publikováno 3. 9. 2012, č. 20(2), s. 123 [cit. 31. 3. 2022]. ISSN 1805-2789. Dostupné z: https://journals.muni.cz/cpvp/article/view/5875/4982.

představují významné interpretační vodítko při výkladu primárního a sekundárního práva EU.

V současné době se jedná především o pokyny, doporučení a postupy, které jsou vydávány Evropským sborem pro ochranu osobních údajů. Úkolem Evropského sboru pro ochranu osobních údajů je především zajištění jednotné aplikace GDPR.[43] Evropský sbor pro ochranu osobních údajů byl zřízen GDPR a nahradil Pracovní skupinu WP29. Přestože měla Pracovní skupina WP29 pouze poradní funkci, byla v období od roku 1997 do roku 2016 uznávaným orgánem. Stanoviska, dokumenty a názory WP29 podstatným způsobem přispěly k formování a interpretaci práva na ochranu osobních údajů.[44]

Dnes již Pracovní skupina nevykonává svou činnost. Z jí vydávaných stanovisek, pracovních dokumentů, pokynů a doporučení je však možné nadále čerpat informace pro lepší pochopení problematiky monitoringu zaměstnanců. Ostatně ze samotného recitálu GDPR vyplývá, že cíle a zásady směrnice nadále platí (bod 9 recitálu GDPR). Dospívám proto k názoru, že by se při studiu problematiky monitoringu zaměstnanců mělo i k těmto nezávazným, ale interpretačně cenným právním aktům přihlížet. Domnívám se, že za zmínku stojí především následující právní instrumenty:

- **Pracovní dokument WP29: Ke sledování elektronických komunikací na pracovišti**. Tento pracovní dokument upravuje otázku monitorování a dohled nad elektronickou komunikací na pracovišti, a to především monitoring elektronické pošty a internetu. Stanovuje podmínky, za kterých může být na zaměstnance aplikováno tajné či nepřetržité sledování. Shodně tak základní podmínky jednotlivých forem monitoringů a jednotlivé povinnosti zaměstnavatelů u těchto konkrétních forem monitoringu. Blíže budou jejich jednotlivé pasáže rozvedeny ve druhé kapitole.
- **Stanovisko WP29 č. 4/2004: Ke zpracování osobních údajů prostřednictvím kamerového sledování**. Jak vyplývá z názvu stanoviska, jeho předmětem je monitoring prostřednictvím

[43] Výčet úkolů sboru je blíže vymezen v článku 70 GDPR. Mezi jeho úkoly se řadí např. poskytování poradenství Komisi ve veškerých záležitostech souvisejících s ochranou osobních údajů v Unii. Přezkoumávat praktické uplatňování pokynů, doporučení a osvědčených postupů či vydávat pokyny, doporučení a osvědčené postupy v souladu s GDPR.
[44] ZAHRADNÍČEK, J. *Ochrana osobnosti v pracovněprávních vztazích*. Praha: Leges, 2019, s. 25. Teoretik. ISBN 978-80-7502-373-5.

kamerového systému a s tím související problematika zpracování osobních údajů. Myslím si, že velmi přínosná je též část 4. tohoto stanoviska, která shrnuje právní úpravu kamerového sledování jednotlivými členskými státy. Tyto informace je však nutné vzhledem ke stáří stanoviska ověřovat. Podrobně také toto stanovisko rozvádí zásadu proporcionality.

- **Stanovisko WP29 č. 8/2001: Zpracování osobních údajů v kontextu zaměstnání**. Za největší přínos tohoto stanoviska spatřuji to, že stanovuje a upravuje základní zásady ochrany údajů, které by měl mít zaměstnavatel při zavádění forem monitoringu vždy na paměti. Mezi tyto základní zásady ochrany osobních údajů zařazuje pracovní skupina především následující zásady: *konečnost, transparentnost, legitimita, proporcionalita, přesnost o uchovávání osobních údajů, zabezpečení nasbíraných osobních údajů* a *splnění informační povinnosti.* Některým z těchto zásad bude bližší pozornost věnována ve třetí kapitole. Zajímavou částí stanoviska je též část, která pojednává o souhlasu zaměstnance. Zde pracovní skupina zdůraznila, že by zaměstnavatelé neměli legitimizovat zpracování osobních údajů souhlasem zaměstnanců a že spoléhání na tento souhlas by se mělo omezit pouze na ty případy, kdy má zaměstnanec skutečně svobodnou volbu a zároveň možnost tento svůj svobodně udělený souhlas bez újmy (např. ztráty zaměstnání) odvolat.

Tyto právní akty lze označit za jakési „manuály“ určené odborné, ale i laické veřejnosti. Dokumenty poskytují přehled o tom, jak má zaměstnavatel postupovat, aby jeho jednání bylo v souladu s GDPR. Kromě toho také poskytují úpravu jednotlivých forem sledování zaměstnanců. Rozsáhlejší pozornost jim bude věnována též ve druhé kapitole.

2 Formy monitoringu

Problematika monitoringu zaměstnance je komplexním tématem. Zaměstnavatel kromě forem a způsobu, kterým bude zaměstnance monitorovat, musí řešit také míru, jakou zasáhne do zaměstnancových práv. Hovoříme zde především o zásahu do práva zaměstnance na soukromý život, který je mu garantován ve čl. 8. Úmluvy.

Vývoj moderních technologií poskytl zaměstnavatelům mnoho nástrojů, které může zaměstnavatel využívat při sledování svých zaměstnanců. Kapitola nastiňuje jak praktickou aplikaci právních předpisů, které byly blíže rozvedeny v předešlé kapitole, tak nejdůležitější aspekty jednotlivých forem monitoringu. Cílem této kapitoly je poskytnout čtenářům z řad laiků i odborníků ucelený přehled v takovém rozsahu, aby mohly být poznatky z této kapitoly využity, jak v rovině akademické, tak praktické.

Kapitola je věnována formám monitoringu, které jsou na pracovišti nejčastěji zaváděny. U každé formy monitoringu je uváděna též relevantní judikatura, a to jak soudů českých, tak soudů mezinárodních, především Evropského soudu pro lidská práva. Rozhodně se nejedná o konečný výčet forem monitoringu, neboť lze do budoucna, a to s ohledem na vývoj informačních technologií i HR trendů očekávat, že těchto forem bude přibývat.

2. 1 Monitoring e-mailové schránky

Při monitorování e-mailů zaměstnanců dochází k interferenci pracovního práva, práva na ochranu osobních údajů reprezentovaného především GDPR, práva na ochranu soukromí garantovaného zaměstnanci Listinou a Úmluvou společně s právem na ochranu vlastnického práva. Poslední ze zmíněných práv svědčí hlavně zaměstnavateli. Typickým projevem pak jsou prostředky, které smí používat výlučně zaměstnavatel, případně zaměstnanec s jeho svolením. Mezi prostředky, které zaměstnanec nesmí bez svolení zaměstnavatele užívat k osobním účelům, řadíme mj. výpočetní techniku. Na výpočetní technice jsou zaměstnanci zpravidla zpřístupněny aplikace, které zaměstnanec využívá pro plnění svých pracovních úkolů. Kromě pracovních úkolů tyto aplikace slouží zaměstnanci také ke komunikaci vně společnosti zaměstnavatele a vůči třetím subjektům mimo zaměstnavatele. K takové komunikaci je velmi často zaměstnanci využívána e-mailová korespondence.

2. 1. 1 E-mail tvořen osobními údaji zaměstnance

Užíváním a monitorováním e-mailové schránky se ve svém Stanovisku č. 2/2009 o ochraně soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště zabýval též ÚOOÚ. ÚOOÚ ve svém stanovisku stanovil, že e-mail složený ze jména a příjmení zaměstnance, tj. například kim.ondrackova@zamestnavatel.cz, je osobním údajem zaměstnance. Na e-mailové zprávy, které budou na tuto adresu zaměstnanci doručeny, je nutno nahlížet jako na soukromou korespondenci, a to i přesto, že e-mailová doména náleží zaměstnavateli. Taková e-mailová adresa bude podléhat ochraně dle zákona o zpracování osobních údajů.

Právo listovního tajemství tedy v tomto případě bude svědčit zaměstnanci. Dle Pomaizlové s Doležalem zaměstnavatel může u takové e-mailové adresy sledovat tok e-mailové korespondence, nikoliv obsah jednotlivých zpráv.[45] ÚOOÚ ve svém stanovisku předestřel podmínky, za kterých může být e-mail doručený na zaměstnavatelovu e-mailovou adresu otevřen. Zaměstnavatel může otevřít e-maily doručené do e-mailové schránky zaměstnance pouze ve výjimečných případech. E-maily mohou být otevírány, bude-li to v zájmu ochrany práv zaměstnavatele. Zaměstnavateli musí být zřejmé, že se jedná o pracovní e-mail. To, že se jedná o pracovní e-mail může zaměstnavateli vyplynout z hlavičky, e-mailové adresy doručovatele či předmětu e-mailové zprávy. U otevírání e-mailů zaměstnance musí být dále pravděpodobné, že z objektivních důvodů by k vyřízení e-mailu zaměstnancem došlo se zpožděním, v jehož důsledku by zaměstnavatel mohl utrpět újmu na svých právech.

Otázka přístupu do e-mailu zaměstnance vyvstává také u přístupu do e-mailu bývalých zaměstnanců. Zvolánek s Malatincovou uvádějí, že do e-mailové schránky bývalého zaměstnance lze vstoupit pouze za konkrétních podmínek. Není přípustné, aby zaměstnavatel mohl svévolně kontrolovat původní či nově doručené e-maily bývalému zaměstnanci. Musí převažovat zájem zaměstnavatele nad právem na ochranu soukromí bývalého zaměstnance. Stejně tak zaměstnavatel nemůže mít možnost využít jiného, byť méně invazivního postupu.[46] Souhrnně lze

[45] POMAIZLOVÁ, K., DOLEŽAL, R. Monitoring emailových zpráv zaměstnanců. *Epravo.cz* [online]. Publikováno 23. 3. 2021 [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/monitoring-emailovych-zprav-zamestnancu-112690.html.

[46] ZVOLÁNEK, J., MALATINCOVÁ, D. Může si zaměstnavatel přečíst e-maily bývalého zaměstnance?. *Epravo.cz*. [online]. Publikováno 15. 7. 2020 [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/muze-si-zamestnavatel-precist-e-maily-byvaleho-zamestnance-111482.html.

tedy uvést, že za legitimní lze označit takovou situaci, kdy zaměstnavatel sice vstoupí do soukromého e-mailu zaměstnance, ale jeho zájmy převáží nad právem na ochranu soukromí bývalého či současného zaměstnance.

Domnívám se, že za legitimní případ by bylo možné označit například situaci, kdy finanční ředitel společnosti bude v důsledku předem neočekávané události (dopravní nehoda, infarkt apod.) dlouhodobě pracovně indisponován. Do jeho e-mailové schránky jsou zasílány faktury. Lze očekávat, že zaměstnanec bude pracovně indisponován i po lhůtě splatnosti těchto faktur. Jejich včasným neuhrazením by se zaměstnavatel dostal do prodlení a musel by hradit i další sankce, např. smluvní pokuty. I v takovém případě však bude muset zaměstnavatel postupovat v souladu s principem proporcionality. Zaměstnavatel bude muset posoudit z hlavičky e-mailu, zda se jedná či nejedná o pracovní e-mail. Teprve až v okamžiku, kdy bude z hlavičky e-mailu patrné, že se jedná o pracovní korespondenci, bude zaměstnavatel oprávněn seznámit se s obsahem tohoto e-mailu. Soukromé e-maily zaměstnavatel nesmí otevírat ani v případě dlouhodobé nepřítomnosti zaměstnance na pracovišti.

2. 1. 2 E-mail bez osobních údajů zaměstnance

E-mail bez osobních údajů jakéhokoliv zaměstnance, tj. například stiznosti@zamestnavatel.cz, je e-mailem úředním. Bez ohledu na to, zda je na něj doručená e-mailová korespondence vyřizována jedním či více zaměstnanci. U takovéto e-mailové adresy bude právo na listovní tajemství svědčit naopak zaměstnavateli. Zaměstnavatel tak zcela oprávněně může příchozí e-mailovou korespondenci na takovou e-mailovou adresu monitorovat, otevírat a vyřizovat. Výjimkou je pouze situace, v níž je na tuto adresu doručena e-mailová korespondence ryze soukromého charakteru. Soukromý charakter došlé korespondence by mohl být shledán například z oslovení, předmětu či e-mailové adresy odesílatele. V takovém případě by zaměstnavatel měl postupovat dle pravidel, která byla uvedena výše. Tedy takovou příchozí e-mailovou korespondenci neotevírat.

Jednou z možností, jak předejít situaci, kdy zaměstnavatel ze závažných důvodů bude muset přistoupit do e-mailu zaměstnance, je nastavení tzv. automatické odpovědi. Automatická odpověď odkáže odesílatele e-mailu v době nepřítomnosti zaměstnance na jiného zaměstnance či kontaktní osobu. Po odcházejícím zaměstnanci lze pak spravedlivě požadovat, aby prostudoval

obsah svého e-mailu a sám zaměstnavateli či jinému zaměstnanci předal svou agendu včetně pracovních e-mailů. Osobně zaměstnavatelům doporučuji nastavení automatické odpovědi také u odcházejících zaměstnanců. Automatická odpověď by měla obsahovat informace o tom, že zaměstnanec skončil a současně kontaktní údaje na jinou osobu, které převzala jeho agendu. Jedná se o preventivní řešení, které může dlouhodobě předcházet případným nesrovnalostem.

2. 1. 3 Doporučení

Myslím si, že zaměstnavateli lze dále doporučit, aby vytvořil obecné e-maily, kam bude směřována nejdůležitější e-mailová korespondence, např. faktury@zamestnavatel.cz, kam budou směrovány veškeré faktury, licence@zamestnavatel.cz, kam budou směrovány jednotlivé přístupy do programů či objednavky@zamestnavatel.cz, kam budou zasílány jednotlivé objednávky. Zaměstnavateli tak bude zajištěn kontinuální přístup do e-mailové schránky i poté, co některý ze zaměstnanců opustí společnost zaměstnavatele. Zaměstnavatel tedy bude mít zajištěn kdykoliv přístup k nejdůležitější korespondenci. Oprávněně mohou být využívány i systémy pro zabránění úniku dat, tzv. *Data Leak Prevention systémy*. Tyto systémy může zaměstnavatel nastavit za účelem kontroly. Cílem kontroly pak bude zjištění, zda zaměstnanec ze své e-mailové adresy nedůvodně a neoprávněně neodesílá třetím osobám citlivá data či soubory.

2. 1. 4 Rozsudek velkého senátu ESLP ze dne 5. září 2017 ve věci 61496/08 – Bărbulescu proti Rumunsku

V tomto případě velký senát ESLP rozhodoval o stížnosti rumunského zaměstnance pana Bărbulescu. Bărbulescu byl propuštěn ze svého zaměstnání z důvodu užití e-mailové korespondence k soukromým účelům. Bărbulescu si na žádost svého zaměstnavatele vytvořil účet u Yahoo Messengeru. Účet si měl pan Bărbulescu založit pro účely rychlejší komunikace s cílovými zákazníky zaměstnavatele. Bărbulescu však měl účet u Yahoo Messenger vytvořen a propojen se svým osobním e-mailem. Zaměstnavatel vnitřním předpisem zakázal zaměstnancům užívat svěřené prostředky k osobním účelům. Zaměstnanci nesměli pro osobní účely užívat počítače, kopírovací zařízení, telefony ani fax. Zákaz se vztahoval též na užívání internetových stránek a aplikací. Dle vnitřního předpisu tedy pan Bărbulescu nesměl užívat Yahoo Messenger k soukromým konverzacím s přáteli, ani svými blízkými.

Zaměstnavatel monitoroval činnost Bărbulescu na internetu a následně ho s výsledky monitorování konfrontoval. Pan Bărbulescu na výsledky reagoval tím, že Yahoo Messenger používal pouze k pracovním účelům. Zaměstnavatel proto předložil Bărbulescovi přepis 45 stran konverzace, kterou si vyměnil se svým bratrem a snoubenkou. Jednalo se o zprávy osobního a intimního charakteru. Na základě tohoto přepisu byl zaměstnavatel panem Bărbulescu nařčen z toho, že porušením listovního tajemství spáchal trestný čin. Zaměstnavatel rozvázal s panem Bărbulescem pracovní poměr.

V rámci své stížnosti Bărbulescu uvedl, že od svého zaměstnavatele nebyl předem upozorněn na to, že by jeho komunikace na účtu Yahoo Messenger mohla být zaměstnavatelem monitorována, ba dokonce čtena. Dále uvedl, že zaměstnavateli za tímto účelem neudělil žádný souhlas. Mimo jiné argumentoval tím, že u účtu Yahoo Messenger byl jedinou osobou, která znala heslo, a proto důvodně očekával zachování soukromí ohledně jeho komunikace. Tvrdil, že zaměstnavatel jeho konverzaci nejdříve po určitou dobu sledoval, a až poté mu dal možnost upřesnit, zda se jedná o komunikaci soukromou či pracovní.

ESLP v předmětném rozhodnutí poznamenal, že e-mail je jednou z forem komunikace umožňující jednotlivcům vést soukromý společenský život. Z toho důvodu je nutné i na odesílání a přijímání e-mailů nahlížet jako na *korespondenci* ve smyslu čl. 8 Úmluvy. V takovém případě není rozhodující ani to, že jsou zprávy zasílány z výpočetní techniky zaměstnavatele.

Velký senát ESLP v předmětném rozhodnutí dále upozornil na to, že je členským státům EU ponechán široký prostor pro přijetí právní úpravy regulující elektronickou či jinou komunikaci zaměstnanců. Podmínky pro oprávnění zaměstnavatelů regulovat korespondenci by měly být individuálně stanoveny jednotlivými státy právě v těchto vnitrostátních předpisech. Není však možné, aby byly možnosti pro vytvoření právního rámce pro členské státy zcela bez omezení. Členské státy by v právní úpravě především měly zohledňovat princip proporcionality a přijmout dostatečné procesní záruky pro to, aby bylo zabráněno zaměstnavatelům svévolně zasahovat do soukromí zaměstnanců. Soudy a jiné vnitrostátní orgány členských států by pak při rozhodování případných sporů měly posuzovat následující faktory:

- **Zda byl zaměstnanec informován o možnosti, že jeho komunikace či korespondence může být zaměstnavatelem monitorována.**

V souvislosti s tímto bodem ESLP uvedl, že pro slučitelnost s článkem 8. Úmluvy musí být zaměstnanec na tuto možnost upozorněn předem. Informace by pro zaměstnance měla být jasná a srozumitelná. Mimo jiné tomuto faktoru odpovídá i další judikatura ESLP. ESLP opakovaně vyjádřil stanovisko, že shromažďování a uchovávání osobních údajů týkajících se elektronické pošty bez vědomí sledovaného, je zásah do práva na respektování rodinného a soukromého života, které garantuje Úmluva v článku 8.[47]

- **Rozsah monitorování ze strany zaměstnavatele a míra zásahu do soukromí zaměstnance.** V úvahu by měly vnitrostátní orgány brát především to, zda byla monitorována veškerá konverzace, nebo pouze její část. Dále by se měly vnitrostátní orgány zabývat také tím, zda bylo monitorování časově omezené či nikoliv. V neposlední řadě by mělo být také zkoumáno, jak velký okruh osob měl přístup k výsledkům monitorování.
- **Zda zaměstnavatel uvedl a měl legitimní důvody pro to, aby mohl korespondenci sledovat a přistupovat k ní.**
- **Zda mohl zaměstnavatel zavést méně invazivní kontrolní mechanismy, než je přímý přístup k obsahu korespondence zaměstnance.**
- **Jaké dopady mělo sledování na zaměstnance, jak byly využity výsledky sledování.**
- **Zda byly poskytnuty zaměstnanci záruky, že sledování probíhá korektním způsobem.**

2. 2 Monitoring aktivity zaměstnance na internetu

Většina zaměstnanců v dnešní době běžně užívá při své práci výpočetní technologie, typicky firemní počítač či notebook. Z tohoto důvodu zaměstnavatelé stále častěji přistupují k monitorování aktivity zaměstnanců na těchto zařízeních. Zaměstnavatel tak např. monitoruje to, jaké stránky zaměstnanci v rámci pracovní doby navštěvují, ale také jejich práci s jednotlivými dokumenty. Tato kapitola se však výhradně zabývá pouze monitoringem aktivity zaměstnanců na internetu.

[47] Rozsudek ESLP ze dne 3. dubna 2007 Coplandová proti Spojenému království, č. stížnosti 62617/00.

U monitoringu aktivity zaměstnanců na internetu se dle Zahradníčka uplatní stejná pravidla jako u dalších forem monitoringu dle § 316 odst. 1 a 2 ZP. Uvádí, že míru zásahu do soukromí zaměstnance bude nutné posuzovat *ad hoc* s ohledem na konkrétní opatření, jež bude zaměstnavatel k monitoringu užívat. Stejně tak bude vždy nutné posuzovat, zda je zvolený kontrolní mechanismus v souladu se zásadou proporcionality a subsidiarity.[48]

Také u této formy monitoringu je ponecháno na vůli zaměstnavatele, zda umožní zaměstnancům užívat internet k soukromým účelům či nikoliv (§316 odst. 1 ZP). Souhlas může být udělen s omezením. Osobně dospívám k obdobnému závěru, jako pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES. Ta dospěla k závěru, že v případě monitorování aktivity na internetu by měl zaměstnavatel před následnou kontrolou přijímat primárně preventivní opatření. Tato preventivní opatření pomohou legálním způsobem předcházet užití internetu zaměstnancem v rozporu s požadavky zaměstnavatele.[49] Současný technologický pokrok totiž zaměstnavatelům poskytuje široké spektrum prostředků a aplikací, jimiž mohou aktivitu zaměstnanců na internetu zamezit.

Murad s Uhrinovou uvádí jako příklad omezení užívání internetu vytvoření tzv. *blacklistů*. Zaměstnavatel zavede automatické blokování určitých webových stránek. Zaměstnanci tak budou předem znepřístupněny sociální sítě, pornografické stránky či stránky s internetovým bankovnictvím. Zaměstnavatel tak předem může zamezit sledování stránek, které představují např. vysoké riziko napadení počítače virem. Výběr blokovaných stránek navíc může zaměstnavatel určovat dle pozice konkrétního zaměstnance. Zaměstnavatel může také naopak určit, jaké stránky budou zaměstnancům zpřístupněny (tzv. *whitelisty*). Může tedy vymezit stránky, u kterých předpokládá, že je bude zaměstnanec ke své práci potřebovat. [50]

Vidrna s Koudelkou ve své publikaci sdělují, že je možné čerpat inspiraci u našich sousedů v Evropské Unii. Jako příklad uvádějí Rakousko, kde je využívána tzv. metoda stupňovitého zajišťování. Cílem této metody je detekce extrémů, resp.

[48] ZAHRADNÍČEK, J. *Ochrana osobnosti v pracovněprávních vztazích.* Praha: Leges, 2019, s. 196. Teoretik. ISBN 978-80-7502-373-5.
[49] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Pracovní dokument o sledování elektronických komunikací na pracovišti (v originále: *Working document on the surveillance of electronic communications in the workplace*) ze dne 29. května 2002, s. 24.
[50] MURAD, M., UHRINOVÁ, A. Monitoring činností zaměstnanců ze strany zaměstnavatele (1. část). *Epravo.cz.* [online]. Publikováno 25. 6. 2019 [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/monitoring-cinnosti-zamestnancu-ze-strany-zamestnavatele-1-cast-109563.html.

extrémního jednání (např. sledování pornografických snímků). Tyto extrémy pak mohou být podrobovány následné bližší kontrole.[51]

2. 2. 1 Doporučení

Myslím si, že pokud zaměstnavatel udělí zaměstnancům souhlas s užíváním internetu k soukromým účelům, měl by též stanovit pravidla, za jakých mohou zaměstnanci internet užívat. Domnívám se, že tato pravidla je nejvhodnější stanovit vnitřním předpisem. Vnitřní předpis by měl být pro zaměstnance jasný a srozumitelný. Mělo by v něm být jasně uvedeno, v jakém časovém úseku může internet k soukromým účelům zaměstnanec využívat (zda po celou pracovní dobu, nebo jen v době obědové pauzy). Dále by měl zaměstnavatel specifikovat, jaký typ stránek může být zaměstnancem navštěvován a jaký nikoliv. Zaměstnavatel by měl také uvést, zda je povoleno stahovat z internetu dokumenty, nebo zda je možné poslouchat muziku. Pokud je souhlas zaměstnavatelem ukládán s omezením, je nutné, aby byl s tímto omezením zaměstnanec dostatečně seznámen. V neposlední řadě by měl zaměstnavatel zaměstnance seznámit také s tím, jak budou využita data, která budou zaměstnavatelem shromážděna. Je totiž žádoucí, aby byl zaměstnanec bezodkladně informován o tom, že používá internet podezřelým způsobem.[52] Zaměstnancům musí být z vnitřního předpisu zřejmý rozsah monitoringu. Zaměstnanci musí být zřejmé, zda se monitoring vztahuje pouze ke konkrétním zaměstnancům či ke všem. Domnívám se, že zaměstnavateli lze též doporučit, aby byl zaměstnanec přezkoušen personalistou, zda vnitřnímu předpisu porozuměl.

2. 2. 2 Monitoring sociálních sítí zaměstnanců

Pod monitoring aktivity zaměstnanců na internetu lze podřadit též sledování jejich aktivity na sociálních sítích. Ty se s rozvojem moderních technologií stávají neodmyslitelnou součástí novodobé společnosti. U monitoringu sociálních sítí zaměstnanců navíc do popředí vystupuje též právo zaměstnance na svobodu projevu. Právo na svobodu projevu je garantováno článkem 17 Listiny. Opomenuto však nemůže být ani právo zaměstnavatele na ochranu dobré pověsti a dobrého jména (čl. 10 odst. 1 LZPS).

[51] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců*. V Praze: C.H. Beck, 2013, s. 131. Beckova edice ABC. ISBN 978-80-7400-453-7.
[52] Pracovní dokument WP29: Ke sledování elektronických komunikací na pracovišti (v originále: *Working document on the surveillance of electronic communications in the workplace*).

Problematické je, jakým způsobem má být posuzována situace, kdy zaměstnanec na svých sociálních sítích sdílí nevhodné příspěvky ze svého soukromého profilu. Otázkou je, zda tyto příspěvky může zaměstnavatel sledovat a případně po jejich vyhodnocení vyvodit pro zaměstnance negativní důsledky či nikoliv. Dle Pravdové není tato problematika dosud českými soudy dostatečně judikována. Inspiraci však lze nalézt v rozhodnutích soudů členských států, a to především v Německu. Německé soudy nevhodné příspěvky vyhodnotily jako důvod pro zrušení pracovního poměru.[53] Podle názoru Pravdové většina zaměstnavatelů vnímá soukromé profily zaměstnanců na sociálních sítích za jejich soukromí, do kterého by nemělo být zasahováno.[54] Sporná však bude například situace, kdy zaměstnanec sdílí příspěvky sympatizující s holocaustem či genocidou. Současně má na stejném soukromém profilu uvedeno, že je zaměstnancem konkrétního zaměstnavatele. Dalším sporným momentem pak budou případy, kdy zaměstnanec ze svého soukromého profilu uráží či hanlivě komentuje profily konkurenčních společností. Zdržet by se měl zaměstnanec též kritických příspěvků vůči zaměstnavateli. Zaměstnavatel má totiž v takovém případě oprávněný zájem na ochraně jeho dobrého jména. Dle Blažka je na zaměstnance kladen požadavek vyšší loajality vůči zaměstnavateli. Sdílení kritiky zaměstnavatele na sociálních sítích může být vyhodnoceno jako jednání v rozporu s oprávněnými zájmy zaměstnavatele na zachování dobrého jména na veřejnosti.[55]

Nejvyšší soud se ve svém rozsudku ze dne 20. 3. 2017, sp. zn. 21 Cdo 1043/2016, zabýval zrušením pracovního poměru zaměstnance. Zaměstnanec pracující ve zpravodajství napsal negativní článek do internetového magazínu. V uveřejněném článku kritizoval jednání svého zaměstnavatele a přirovnával jeho postupy k totalitnímu režimu. Obsah zpravodajství byl totiž před každým odvysíláním cenzurován a schvalován vlastníkem média a generální ředitelkou. Zaměstnanec s tímto cenzurováním nesouhlasil a odmítal obsah zpravodajství ke schválení zasílat. Důvody pro své chování i nesouhlas s cenzurou a schvalovacím procesem sdělil e-mailem též generální ředitelce.

[53] PRAVDOVÁ, M. Sociální média na pracovišti. *Právní prostor.* [online]. Publikováno 21. 5. 2018. [cit. 31. 3. 2022]. Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/socialni-media-na-pracovisti.
[54] Tamtéž.
[55] BLAŽEK, V. Kritika zaměstnavatele na sociálních sítích jako důvod pro skončení pracovního poměru. *Epravo.cz.* [online]. Publikováno 7. 1. 2016 [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/kritika-zamestnavatele-na-socialnich-sitich-jako-duvod-pro-skonceni-pracovniho-pomeru-99663.html.

Soud v daném rozsudku judikoval, že svoboda projevu zakotvená Listinou není absolutní. Uvedl, že proti svobodě projevu stojí i jiné oprávněné zájmy, a to včetně oprávněných zájmů zaměstnavatele. Zároveň stanovil, že aby bylo možné požadovat kritiku za oprávněnou, musí splňovat následující charakteristiky. Musí být:

- **věcná,** tzn. je vyžadováno, aby byla založena na pravdivých skutkových tvrzení.
- **konkrétní**
- **přiměřená**, co do obsahu, formy i místa, tj. nesmí se jednat o kritiku přehnanou.

Přihlíženo však vždy bude muset být ke konkrétním okolnostem. V případě, že kritika vybočí z mezí přípustnosti, stejně tak jako je tomu v tomto případě, převáží ochrana dobré pověsti a jména zaměstnavatele před právem zaměstnance na svobodný projev. Rozsudek Nejvyššího soudu byl následně potvrzen usnesením Ústavního soudu ze dne 16. 8. 2017, sp. zn I. ÚS 1716/17. Ústavní soud v odůvodnění usnesení dále uvedl, že se zaměstnanec měl primárně se svým podnětem obrátit na Radu pro rozhlasové a televizní vysílání.[56]

Dospívám k závěru, že zaměstnavatelům lze doporučit, aby přijali etický kodex, v němž mohou být stanovena pravidla zaměstnanců pro chování na sociálních sítích. Jako příklad uvádím společnost KONE, a.s., která poskytuje především služby spojené s výtahy, eskalátory apod. Zaměstnanci této společnosti by dle etického kodexu neměli sdílet či ukládat informace o této společnosti na sociálních sítích. Zaměstnanci by dále neměli ani publikovat obchodní tajemství či jiné utajované informace. Kromě toho by v případě veřejného doporučování služeb či produktů této společnosti, měli třetí osoby vyrozumět o tom, že jsou zaměstnanci této společnosti.[57]

[56] GORČÍK, J. Porušení povinností zaměstnance ve světle judikatury Nejvyššího soudu aneb šance pro zaměstnavatele při sporech se zaměstnanci. *Právní prostor.* [online]. Publikováno 1. 10. 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/poruseni-povinnosti-zamestnance-ve-svetle-judikatury-nejvyssiho-soudu-aneb-sance-pro-zamestnavatele-pri-sporech-se-zamestnanci.

[57] KONE.com. *Etický kodex společnosti KONE*. [online]. Publikováno září 2021 [cit. 31. 3. 2022]. Dostupné z: https://www.kone.com/fi/Images/KONE-Code-of-Conduct-Czech_tcm18-68547.pdf.

2. 2. 2 Rozsudek Nejvyššího soudu České republiky ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011

Nejvyšší soud v tomto případě rozhodoval o neplatnosti výpovědi. Zaměstnavatel se zaměstnancem okamžitě zrušil pracovní poměr. Jako důvod zaměstnavatel uvedl zvlášť hrubé porušení povinností. Toto zvlášť hrubé porušení povinností zaměstnavatel spatřoval v tom, že zaměstnanec v pracovní době strávil 102,97 hodin neefektivní prací na počítači. Zaměstnanec však namítal, že zaměstnavatel tajně sledoval užívání internetu a jednal tak v rozporu s ust. § 316 odst. 2 ZP. Pro úplnost je nutno uvést, že bylo zaměstnancům pracovním řádem zakázáno navštěvovat stránky s citlivým obsahem i stránky typu on-line zpravodajství. Zaměstnanci dále nesměli využívat internet k poslechu rádiových stanic či sledování pořadů a filmů.

Nejvyšší soud v daném případě dospěl k názoru, že ze strany zaměstnavatele nešlo o skryté sledování ve smyslu § 316 odst. 2 ZP. Zaměstnavatel v rámci kontroly sice sledoval pohyb zaměstnance na internetu a jiných stránkách, avšak bez toho, aby byl monitorován a zpracováván obsah těchto stránek. Nejvyšší soud dále v rozhodnutí uvedl, že *nebyly činěny záznamy projevů osobní povahy.*

Nejvyšší soud se v rozhodnutí dále zabýval pojmem *přiměřená kontrola*. Vzhledem k tomu, že zákon blíže nestanovuje, co je *přiměřeností kontroly* míněno. Soud stanovil, že ustanovení § 316 odst. 1 ZP je právní normou s relativně neurčitou hypotézou. Hypotézu tudíž nestanovuje přímo právní předpis, ale je ponecháno na uvážení soudu, aby v konkrétním případě tuto hypotézu vymezil. Dle Nejvyššího soudu lze předpokládat, že soudy budou tuto hypotézu interpretovat především s ohledem na to, zda se jednalo o kontrolu průběžnou či následnou. Vyhodnocovat budou především délku kontroly, její rozsah, ale také to, zda kontrola zaměstnance omezovala a zasáhla do jejich práva na soukromí či nikoliv. Opomenut by neměl být ani přezkum takového zásahu do tohoto práva.

Zaměstnavatel využil kontroly pouze za tím účelem, aby zjistil, zda zaměstnanec respektoval zákaz užívat pro osobní potřebu svěřené prostředky společně se zákazem, který mu byl nad rámec zákonné úpravy stanoven vnitřním předpisem. Soud tedy v tomto případě rozhodl tak, že prováděná kontrola směřovala k ochraně zaměstnavatele.

O soukromí zaměstnance a jeho osobnosti zajisté vypovídá také to, jaké webové stránky navštěvuje. Toto však nebylo podstatou předmětné kontroly. Účelem kontroly bylo pouze zjištění, zda zaměstnanec sledoval internetové stránky, které nesouvisely s výkonem jeho práce či nikoliv. Kontrola zaměstnavatele tedy byla v tomto konkrétním případě legitimní. Směřovala k ochraně majetku zaměstnavatele a nebylo při ní narušeno soukromí zaměstnance.

Zajímavým zahraničním judikátem je rozhodnutí německého federálního pracovního soudu ze dne 27. července 2017, sp. zn. 2 AZR 681/16. V tomto případě soud rozhodoval o rozvázání pracovního poměru se zaměstnancem, který pracoval na pozici webového vývojáře. Na svém pracovním počítači trávil své přestávky prací pro svého otce. Práci soukromého charakteru odváděl maximálně 10 % své pracovní doby. Zbylých minimálně 90 % své pracovní doby se již věnoval pouze pracovním projektům. Zaměstnavatel monitoroval své zaměstnance prostřednictvím *keyloggeru*.[58] Pracovní soud zde v bodě 24. uvedl, že otevřeným užitím keyloggeru dochází k porušení práva na informační sebeurčení, které je součástí práva na ochranu soukromí. V daném případě nebyla naplněna zásada proporcionality. Keylogger by měl být zaměstnavatelem nasazován především v situacích, kdy má zaměstnavatel podezření, že jeho zaměstnanec páchá trestný čin. V důsledku toho, pak může být záznam z keyloggeru užit jako důkaz pro rozvázání pracovního poměru.

2. 3 Monitoring firemního telefonu zaměstnance

Dalšími hojně využívanými přístroji svěřenými zaměstnancům jsou telefony. Firemní telefony, které jsou svěřeny zaměstnanci zaměstnavatelem, nemohou být bez souhlasu zaměstnavatele užívány k soukromým účelům. ÚOOÚ ve svém stanovisku[59] formuloval dva důvody, pro které je zaměstnavatel oprávněn pořizovat záznamy telefonických hovorů svých zaměstnanců. Za první označil situaci, kdy zaměstnavatel zpracovává tyto hovory, protože je to nezbytné pro plnění smlouvy, reklamaci případných vzniknuvších vad či odstoupení od smlouvy. Bude se tak jednat například o situaci, kdy zaměstnanec pracuje na pozici operátora call centra. Na této pozici zaměstnanec uzavírá se třetími osobami objednávky na

[58] Keylogger představuje druh software, který sleduje stisky kláves. Díky tomu může zaměstnavatel získat veškeré informace, které zaměstnanec na svém počítači napíše, včetně hesel, osobních informací či uživatelských jmen do jednotlivých aplikací apod.
[59] ÚOOÚ: Stanovisko č. 5/2013: Pořizování hlasových záznamů v rámci elektronické komunikace při poskytování služeb z pohledu zákona o ochraně osobních údajů. Říjen 2013, s. 2-3.

určité služby či zboží. V takovém případě bude převažovat chráněný zájem zaměstnavatele nad zájmem zaměstnance.

Druhým důvodem bude skutečnost, kdy zaměstnavatel nahrává telefonické hovory s klienty zaměstnanců za účelem zvyšování kvality jím poskytovaných služeb. Zpracování osobních údajů zaměstnanců je pak za účelem zvyšování kvality služeb dle ÚOOÚ možné provádět bez souhlasu zaměstnance. Vidrna s Koudelkou ve své publikaci uvádějí, že záznam telefonních hovorů těchto zaměstnanců je velice významný z hlediska zpětné kontroly. Tyto hovory mohou sloužit jako jediný nástroj, kterým lze zpětně vyhodnotit správnost řešení problému, případně korektnost poskytnuté informace, na jejímž základě byla závazná objednávka zboží či služeb učiněna.[60] I v této situaci musí zaměstnavatel postupovat tak, aby jeho jednání nebylo v rozporu s právem zaměstnance na ochranu jeho soukromého a osobního života. Zaměstnavatel nebude nikdy oprávněn odposlouchávat soukromé telefonní hovory zaměstnance. Soukromé telefonní hovory není možné monitorovat ani v případě jejich uskutečnění během pracovní doby za pomocí telefonu svěřeného zaměstnanci zaměstnavatelem.[61] Obsah takových hovorů i SMS zpráv podléhá ochraně dle trestního zákoníku a Listiny.[62] Zaměstnavatel tedy může například kontrolovat výpis z telefonních hovorů. Z tohoto výpisu telefonních hovorů může snadno zjistit, na jaká telefonní čísla zaměstnanec volal. Nemůže však monitorovat obsah těchto hovorů. Následné prokazování toho, zda zaměstnanec vedl hovor soukromý či pracovní však může být složité. Kupříkladu náborář v personální agentuře může udělat desítky hovorů denně. Navrhuji zaměstnavateli řešení, aby formuloval pravidla užívání firemních telefonů, nebo je případně zakázal užívat pro soukromé účely, a to vnitřním předpisem. V případě, že je tato povinnost zaměstnancům stanovena, jsou povinni ji bez dalšího respektovat. Užije-li zaměstnanec firemní telefon i přes zákaz stanovený vnitřním předpisem k soukromým účelům, bylo by možné za výše uvedených okolností na takové jednání nahlížet jako na porušení povinnosti zaměstnance. Toto jednání by mohlo být dále posouzeno jako porušení pracovních povinností zaměstnancem. Zaměstnavatel by pak také mohl po zaměstnanci uplatňovat nárok na náhradu škody dle zákoníku práce.

[60] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců.* V Praze: C.H. Beck, 2013, s. 102. Beckova edice ABC. ISBN 978-80-7400-453-7.
[61] JOUZA, L. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. *Bulletin advokacie*. 2014, č. 6, s. 29. ISSN 1210-6348.
[62] Tamtéž.

2. 3. 1 Rozsudek Nejvyššího soudu ze dne 7. 8. 2014, sp. zn. 21 Cdo 747/2013

Nejvyšší soud České republiky se v daném rozhodnutí zabýval určením neplatnosti výpovědi z pracovního poměru. Zaměstnavatel dal zaměstnanci výpověď na základě neuspokojivých pracovních výsledků. Neuspokojivé pracovní výsledky byly spatřovány mj. v tom, že zaměstnanec na internetu v průběhu tří pracovních dnů během pracovní doby vyhledával informace pro své soukromé účely. Dále také zaměstnanec pro soukromé účely v období téměř jednoho měsíce zneužíval firemní telefon, když uskutečnil 84 soukromých hovorů.

Soud ve svém rozhodnutí odkázal na ustanovení § 316 odst. 1 ZP, které ve větě druhé stanovuje oprávnění zaměstnavatele přiměřeným způsobem kontrolovat, zda zaměstnanci dodržují zákaz užívat výrobní a pracovní prostředky zaměstnavatele pro osobní potřebu. Soud zde rozhodl, že v dané věci cíleným monitoringem nechtěl zaměstnavatel zjišťovat obsah telefonátů svého zaměstnance. Zaměstnavatel si v tomto případě chtěl pouze ověřit, zda zaměstnanec dodržuje stanovený zákaz užívat svěřené prostředky k soukromým účelům. Když zaměstnavatel dospěl k závěru, že zaměstnanec tento zákaz porušuje, bylo jeho druhotným cílem zjistit, v jaké intenzitě je zákaz porušován. Domnívám se, že pokud by zaměstnanec užil firemní telefon např. 4x, zaměstnavatel by toto mohl ještě akceptovat a vyřešit celou situaci upozorněním zaměstnance na porušení povinnosti. Obzvláště u mobilních telefonů, které jsou přizpůsobeny na dvě SIM karty, se velmi lehce stane, že zaměstnanec nedopatřením zavolá z pracovního čísla. Zde však zaměstnanec užil i přes výslovný zákaz mobilní telefon k 84 soukromým hovorům. O nedopatření tedy v tomto případě zajisté nešlo.

Domnívám se, že závěry soudu lze shrnout do následujícího pravidla. Za přiměřenou lze označit takovou kontrolu, jejímž účelem bude posouzení, zda zaměstnanci dodržují zákaz užívat výrobní či pracovní prostředky zaměstnavatele pro osobní potřebu. V takovém případě totiž zaměstnavatel bude kontrolovat ty povinnosti, které jím nebyly vyloučeny či zmírněny. Zaměstnavateli lze i přesto doporučit, aby při monitoringu firemních telefonů svých zaměstnanců postupoval obezřetně a minimalizoval příležitost, že se seznámí s obsahem telefonátů.

2. 3. 2 Rozsudek Okresního soudu v Mělníku ze dne 11. 2. 2021, sp. zn. 6 C 306/2019

Jak bylo uvedeno výše, zaměstnanec nesmí bez souhlasu zaměstnavatele používat firemní mobilní telefon k soukromým účelům. V případě, kdy telefon i přes předešlý zákaz použije, může po něm zaměstnavatel vymáhat náhradu škody, která mu tímto užíváním telefonu vznikla.

Takovým případem se zabýval i Okresní soud v Mělníku. V daném rozhodnutí byl předmětem sporu nárok zaměstnavatele na peněžité plnění. Zaměstnankyni byla svěřena SIM karta s měsíčním paušálem na 200 volných minut a 70 SMS. Zaměstnankyně byla seznámena s vnitřním pokynem, který stanovoval pravidla pro užívání služebních mobilních telefonů. Vnitřním pokynem bylo mj. stanoveno, že firemní telefony mají být užívány výlučně k plnění pracovních povinností. Zaměstnanec, který překročil tento paušální limit, byl dle pokynu povinen zaměstnavateli uhradit nedoplatek. Nedoplatek měl být hrazen na pokladně zaměstnavatele, a to na základě čtvrtletního vyúčtování. Zaměstnanec nebyl povinen nedoplatek zaměstnavateli platit, pokud prokázal, že k překročení paušálního limitu došlo v souvislosti s plněním pracovních povinností.

Zaměstnankyně stanovený paušální limit překročila. Z výpisu telefonních hovorů navíc bylo možné identifikovat, že pouze tři hovory byly uskutečněny s nadřízeným zaměstnankyně. Pouze nadřízený přitom uděloval zaměstnankyni úkoly. Hovory byly navíc z telefonního čísla uskutečňovány též v době, kdy byla zaměstnankyně v pracovní neschopnosti. Soud v daném případě dospěl k závěru, že zaměstnankyně nepoužívala svůj služební telefon v souladu s vnitřním pokynem, a to výlučně k plnění pracovních povinností. Soud proto zaměstnankyni uložil povinnost uhradit zaměstnavateli jím vymáhanou částku.

Jak již bylo uvedeno výše, lze všem zaměstnavatelům doporučit, aby byla pravidla pro užívání firemních telefonů určena minimálně vnitřním předpisem. Domnívám se, že takový vnitřní předpis by měl být jasný, srozumitelný a koncipovaný tak, aby byl pro zaměstnance přehledný a pochopitelný. Za praktické lze označit také řešení, kdy zaměstnavatel umožní zaměstnanci užívat firemní telefon k osobním účelům a zajistí zaměstnancům firemní tarif. Zaměstnancům bude stanoven konkrétní limit. V situaci, kdy zaměstnanci limit překročí, budou povinni tento rozdíl zaměstnavateli zaplatit. Zaměstnavatel tak nebude nucen zasahovat do soukromí svých zaměstnanců. Zaměstnavatel pouze vždy koncem

měsíce vyhodnotí, zda došlo k překročení limitu či nikoliv. Takové vyhodnocení přitom může provádět bez toho, aniž by monitoroval, na jaká telefonní čísla zaměstnanec volal.

Zaměstnavateli lze též doporučit možnost vytvořit seznam telefonních čísel, na které zaměstnanec může volat bez omezení. Toto řešení by bylo vhodné pro situace, kdy bude zaměstnanec mobilní telefon užívat primárně pro potřeby komunikace se svými kolegy a nadřízenými. Další možností je určit jako povinnost, aby byly prioritně užívány na pracovišti pevné linky. Shodně tak lze zaměstnavateli doporučit, aby ve vnitřním předpise uvedl, na jaká čísla zaměstnancem nesmí být voláno. Jako příklad lze uvést různé zpoplatněné linky, např. telemarketing.

2. 3. 3 Rozsudek ze dne 25. června 1997 ve věci 20605/92 – Halford proti Spojenému království

Obdobný názor zastává ve své rozhodovací praxi i ESLP. V rámci tohoto rozhodnutí ESLP stanovil, že odposlech telefonních hovorů zaměstnance je porušením článku 8 Úmluvy. Uvádí, že není rozhodující, zda byl hovor uskutečněn během pracovní doby či nikoliv. Dále uvádí, že není podstatné, zda byl hovor uskutečněn z firemního telefonu. Hovory z pracoviště i z domova totiž dle názoru ESLP spadají pod pojmy *soukromý život* a *korespondence*. Pod pojmem korespondence si nelze v dnešní technologicky pokročilé době představit pouze korespondenci v listinné podobě. Pojem korespondence totiž zahrnuje i telefonní hovory, elektronickou komunikaci přijatou na pracovišti či doručenou z pracoviště, dále e-maily přijaté nebo odeslané z pracovního počítače.

2. 3. 4 Nález ÚS České republiky ze dne 9. prosince 2014, sp. zn. II. ÚS 1774/14

Další významné stanovisko týkající se monitoringu zaměstnanců se nachází v nálezu Ústavního soudu ze dne 9. prosince 2014, sp. zn. II. ÚS 1774/14. Ústavní soud zde rozhodoval o ukončení pracovního poměru pro nadbytečnost. Dle úsudku zaměstnance však nedošlo k ukončení pracovního poměru pro nadbytečnost, ale z důvodu kritiky. Zaměstnanec totiž na mezinárodním veletrhu během konverzace s členem zahraničního vedení vyjádřil svůj kritický názor na společnost, pro kterou pracoval na pozici technického a obchodního zástupce. Zaměstnanec na podporu svého tvrzení v rámci řízení před Městským soudem v Brně předložil přepis překladu této konverzace mezi zaměstnancem a členem zahraničního vedení a audiokazetu. Ústavní soud rozhodoval o tom, zda byl provedený důkaz

audionahrávkou přípustný či nikoliv. Prostřednictvím testu proporcionality musel posoudit kolizi základních práv a svobod. V daném případě kolizi mezi zájmem na ochranu osobnosti toho, jehož projev byl zachycen bez jeho souhlasu na prováděné audionahrávce, a zájmem na ochranu práv stěžovatele jako zaměstnance.

Ústavní soud následně dospěl k závěru, že v tomto případě představovala předkládaná audionahrávka jediný přímý důkaz. Odkázal zároveň na straně 8. tohoto rozhodnutí na *princip konstitucionalizace ochrany slabší strany*. Tento princip by měly mít soudy při vedení dokazování stále na zřeteli. V oblasti pracovního práva je nutné v soudním řízení o ukončení pracovního poměru chránit zaměstnance před jakýmikoli formami nátlaku a svévole ze strany zaměstnavatele. V případě, kdy by soud v rámci řízení tento princip neaplikoval, poskytovaná ochrana by dle Ústavního soudu byla pouze formální a pro zaměstnance neúčinnou. Zaměstnanec je totiž v rámci pracovněprávního vztahu slabší stranou.

V daném případě totiž stál za zásahem do soukromí nahrávané osoby (člen vedení společnosti) ospravedlnitelný zájem slabší strany (zaměstnanec). Zaměstnanci hrozila závažná újma (např. ztráta zaměstnání). Tedy v daném případě tak byl dle ÚS důkaz užit zaměstnancem zcela legitimně. Tento názor vyjadřuje též Nejvyšší soud ve svém rozsudku ze dne 11. května 2005, sp. zn. 30 Cdo 64/2004. Nejvyšší soud zde stanovil, že hovory fyzických osob při výkonu povolání na pracovišti (nebo při obchodní činnosti) zpravidla nemají projevy osobní povahy. V občanském řízení je tedy možné provést jako důkaz zvukový záznam takových rozhovorů.

2. 4 Monitoring prostřednictvím GPS lokalizátorů

Dalším z nástrojů, které zaměstnavatelé využívají ke kontrole svých zaměstnanců, jsou GPS lokátory. Tento druh technologií najde své uplatnění především u zaměstnavatelů, kteří potřebují mít přehled o pohybu svých zaměstnanců. Konkrétně hovoříme o povoláních, jako je například kurýr či obchodní zástupce. Údaje získané GPS lokátory jsou osobními údaji ve smyslu čl. 4 GDPR.

Prostřednictvím GPS lokátorů zaměstnavatelé získávají údaje o trase svých zaměstnanců. Mezi tyto údaje lze řadit kupř. údaj o geolokaci firemního vozidla a zaměstnance, ale též údaje o způsobu řízení zaměstnance či ujetou vzdálenost. Osobními údaji jsou také data shromážděná kamerami umístěnými ve firemním

automobilu.[63] Z těchto údajů je zaměstnavatel schopen přímo či nepřímo identifikovat konkrétní zaměstnance. Prostřednictvím GPS lokátorů zaměstnavatelé často sledují jízdu propůjčeného firemního vozidla. Jízdu může zaměstnavatel sledovat prostřednictvím nepřímého monitoringu, a to umístěním GPS lokátoru v automobilu. Dále můžu využít možnost přímého monitoringu, kterým sleduje přímo pohyb svého zaměstnance, zpravidla umístěním GPS lokátoru na firemní oblečení zaměstnance.

Také monitoring prostřednictvím GPS lokalizátorů musí být v souladu se zásadou proporcionality a subsidiarity. Zaměstnavatel může tento druh monitoringu zavést pouze za předpokladu, že bude mít pro takový monitoring závažný důvod. Kadlecová tento důvod spatřuje např. u zaměstnavatele, který se potýká s černými jízdami svých zaměstnanců. Taková situace může nastat např. u zaměstnavatele, který má vozový park vybaven několika vozidly. Současně přístup k těmto vozidlům má větší množství zaměstnanců. Závažný důvod bude dle Kadlecové dále naplněn u zaměstnavatelů, kteří se potýkají s častými krádežemi služebních vozidel.[64] Kromě toho bude tento závažný důvod také shledán v případě, že bude zaměstnanec zaměstnavatelem sledován za účelem zajištění bezpečnosti zaměstnance či zboží, které zaměstnanec převáží. Jednalo by se tedy např. o pracovníky, kteří převáží ceniny nebo peníze.

Zaměstnavatel musí vždy důsledně vyhodnocovat, zda není možné k zajištění bezpečnosti využít i jiných, méně invazivních mechanismů. Takto by měl postupovat především v případě, kdy bude jako jediný z důvodů pro zavedení monitoringu GPS lokalizátory zaměstnavatelem označeno zajištění bezpečnosti zaměstnanců. Zaměstnavatel musí nejdříve využít mechanismy, které zasahují do soukromí zaměstnance méně než GPS lokátory. Mezi takové mechanismy se řadí např. omezovače rychlosti, systém záchranného brždění či instalace systému blokujícího telefonování za volantem.[65]

---

[63] Pokyn Evropského sboru pro ochranu osobních údajů č. 01/2020 ke zpracování osobních údajů v souvislosti s propojenými vozidly a aplikacemi souvisejícími s mobilitou verze 2.0. (v originále: *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*) ze dne 9. března 2021, s. 4.

[64] KADLECOVÁ, T. GPS ve služebních vozidlech aneb malý čip = velká komplikace?. *Praktická personalistika*. Sagit, 2015, 2015(3-4/2015).

[65] VRBÍKOVÁ, B. Stanovisko Pracovní skupiny 29 k monitorování zaměstnanců na pracovišti i mimo něj. *Epravo.cz*. [online]. Publikováno 13. 9. 2017. [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/stanovisko-pracovni-skupiny-29-k-monitorovani-zamestnancu-na-pracovisti-i-mimo-nej-106342.html.

Dospívám k závěru, že v případě, kdy si zaměstnavatel stanoví jako důvod zaváděného monitoringu ochranu zdraví svých zaměstnanců, měl by volit mechanismy nejefektivnější a nejvhodnější vzhledem k účelu. Osobně se domnívám, že v konkrétní život ohrožující dopravní situaci je systém záchranného brždění pro ochranu zdraví a života zaměstnance i třetích osob mnohem přínosnější. Pokročilé GPS lokalizátory sice dokáží vyhodnocovat řízení zaměstnance včetně jeho rychlosti, nicméně vůči případné nehodě působí spíše pasivně. Pracovní skupina dále např. dospívá k závěru, že nadbytečný bude monitoring zaměstnanců prostřednictvím GPS lokalizátorů též v případech, kdy si zaměstnanec může organizovat své pracovní cesty dle svých představ.[66]

Informační povinnost musí být zaměstnavatelem splněna také u monitoringu firemních vozů prostřednictvím GPS lokátorů. Informováni by měli být zaměstnanci nejen o tom, že je nainstalován kontrolní mechanismus, ale také o tom, že může být sledováno a vyhodnocováno jejich řidičské chování. Typicky je vyhodnocováno dodržování bezpečnostních přestávek[67] a dodržování pravidel silničního provozu[68]. Pracovní skupina zaměstnavatelům doporučuje, aby u každého firemního vozidla umístili takovou informaci viditelně v zorném poli řidiče.[69]

Radičová k monitoringu prostřednictvím GPS lokalizátorů dále uvádí, že je nutné, aby zavedený monitoring svým rozsahem a intenzitou představoval sledování ve smyslu § 316 odst. 2 ZP. Podle Radičové musí být takový monitoring *intenzivní, soustavní a dlouhodobý*. V případě, kdy zaměstnavatel bude GPS využívat v krátkém časovém intervalu, a to např. za účelem zefektivnění vytíženosti jednotlivých dopravních linek či optimalizace, nebude se na takové jednání ust. § 316 odst. 2 ZP vztahovat.[70]

---

[66] Stanovisko WP29 č. 5/2005: k užívání lokačních údajů s přihlédnutím k poskytování služeb s přidanou hodnotou. (v originále: *Opinion on the use of location data with a view to providing value-added services*) ze dne 25. listopadu 2005, s. 10.

[67] Úprava bezpečnostních přestávek je obsažena v Nařízení vlády č. 168/2002 Sb., kterým se stanoví způsob organizace práce a pracovních postupů, které je zaměstnavatel povinen zajistit při provozování dopravy dopravními prostředky.

[68] Zákon č. 361/2000 Sb., zákon o provozu na pozemních komunikacích a o změně některých zákonů.

[69] Stanovisko WP29 č. 2/2017: ke zpracování osobních údajů na pracovišti (v originále: *Opinion 2/2017 on data processing at work*) ze dne 8. června 2017, s. 17.

[70] RADIČOVÁ, Z. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy*, 2014, č. 21, s. 736-740.

2. 5 Monitoring firemního vozidla, které je zaměstnanci svěřeno k osobním účelům

Umožní-li zaměstnavatel zaměstnanci užívat firemní vozidlo k soukromým účelům, měl by být zaměstnanci k dispozici systém, který umožní vypnutí sledování polohy mimo pracovní dobu. Konkrétně hovoříme o případech, kdy by potenciální sledování mohlo být pro zaměstnance zvláště invazivním zásahem do jeho soukromé sféry.[71] Typicky se bude jednat například o návštěvu zdravotnických zařízení či vyzvedávání dětí ze školy. Dospívám totiž k závěru, že si žádný zaměstnanec nepřeje, aby jeho zaměstnavatel věděl o tom, jaké lékaře navštěvuje. Jako informaci osobní povahy spatřuji též místo, kde studují jeho děti. Konkrétní práva a povinnosti o užívání firemních vozidel pro soukromé účely jsou zpravidla upraveny v dohodě o použití firemního vozidla.

Za předpokladu, že je zaměstnanci uložen souhlas s užíváním firemního vozidla k soukromým účelům, je zaměstnavatel ve shromažďování údajů limitován. Někteří zaměstnavatelé jsou natolik benevolentní, že umožňují zaměstnancům užívat firemní vozidla i pro soukromé dálkové trasy. V takových případech by měly být GPS lokátory vozu vypnuté. Zaměstnavatel by v takovém případě neměl shromažďovat údaje o cestě zaměstnance. Domnívám se, že také údaje o cestě, ubytování nebo stravování patří mezi osobní informace. Dospívám tedy k názoru, že by takové shromažďování údajů bylo vyhodnoceno jako jednání v rozporu s právními předpisy. Naproti tomu si myslím, že by zaměstnavatel za účelem ochrany před krádeží vozidla mohl jednorázově ověřit, zda se zaměstnancovo vozidlo nachází na místě předem oznámeném.

Výjimkou by byla dále situace, za které by proporcionalita byla přiměřená hrozícím rizikům.[72] Např. za předpokladu, že by monitoring sloužil k ochraně vlastnického práva zaměstnavatele, by bylo možné nastavit GPS lokátor tak, aby poloha vozidla začala být sledována v případě, kdy se vozidlo začne pohybovat mimo území České republiky.[73] V takovém případě lze očekávat, že by ochrana zaměstnavatele před krádeží firemního vozidla převážila nad ochranou soukromí zaměstnance mimo rámec pracovní doby. Opět však pouze za předpokladu, že by

[71] Tamtéž.
[72] Tamtéž.
[73] Tamtéž.

zaměstnanec, kterému bylo vozidlo svěřeno k soukromým účelům i k cestám do zahraničí, zaměstnavateli nenahlásil, že se bude s vozidlem pohybovat v zahraničí.

2. 5. 1 Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 3. července 2013, sp. zn. UOOU-00237/13

Média se v minulosti intenzivně věnovala kauze České pošty, a.s., která v době od 1. března 2012 do 6. února 2013 prostřednictvím GPS lokalizátorů (tzv. *trackerů*) zpracovávala vyjma údajů o doručovacích místech v rozsahu místa a času, taktéž osobní údaje doručovatelů. Tato data měla být monitorována za účelem optimalizace okrsků a využita k následnému zlepšení jejich vytíženosti. Dalším vytyčeným účelem monitoringu bylo zajištění rovných pracovních podmínek pro doručovatele. Data měla být užita k minimalizaci diametrální vytíženosti doručovatelů na jednotlivých okrscích. Kromě toho měl monitoring přispět také k vylepšení reklamačního řízení. Nasbíraná data představovala především délku trasy doručovatele, času jím na této trase stráveného a trasu doručovatelem prošlou. Česká pošta, a.s. dále z těchto dat měla vyhodnocovat, zda se doručovatel pohyboval na své trase, která mu byla zaměstnavatelem určena.

Pohyb zaměstnanců nebyl vyhodnocován či sledován v pracovní době, ale byl pořizován záznam zpětně. Dle názoru zástupců České pošty, a.s. byly pořízené záznamy ukládány tak, aby došlo k maximální možné anonymizaci osobních údajů doručovatelů. Zaměstnanci navíc mohli sledovací systém vypínat v okamžiku, kdy čerpali přestávku. Jak již bylo uvedeno výše, Česká pošta, a.s. své zaměstnance tímto způsobem sledovala v časovém úseku téměř jednoho roku.

ÚOOÚ v daném případě shledal, že monitoring představoval nepřiměřený a závažný zásah do soukromí zaměstnanců. Vyjádřil stanovisko, že monitoring neodpovídal účelům, které si Česká pošta, a.s. stanovila. ÚOOÚ uvedl, že pro zajištění optimalizace poskytovaných služeb postačilo sledování kratšího trvání s následným vyhodnocením. Česká pošta, a.s. však sledovala své zaměstnance téměř rok. Pro vyřizování reklamací spolu s vylepšováním doručovacích služeb pak dle ÚOOÚ měl České poště, a.s. postačit údaj o doručovacích místech v rozsahu místa a času. Ze shora uvedených důvodů proto ÚOOÚ uložil České poště, a.s. pokutu ve výši 80 000 Kč. Česká pošta, a.s. však i přes rozhodnutí ÚOOÚ stále zastávala názor, že v daném případě nešlo o zpracování osobních údajů, ale pouze o ukládání a zaznamenávání dat ryze statistické povahy.

2. 5. 2 Rozsudek Městského soudu v Praze ze dne 5. května 2017, sp. zn. 6 A 42/2013

Česká pošta, a.s. se po (z jejího pohledu) neúspěšném rozkladu obrátila se správní žalobou na Městský soud v Praze. Zde opět argumentovala tím, že se na ní jako na poskytovatele služby ve veřejném zájmu (konkrétně poskytování poštovních služeb), vztahuje povinnost ve smyslu čl. 13 LZPS a § 16 zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů. Česká pošta, a.s., je povinna zachovávat mlčenlivost o skutečnostech, které se dozví v souvislosti s výkonem poštovních služeb. Od této povinnosti Česká pošta, a.s. dovozovala, že disponovala důvody zvláštního zřetele hodného, pro které byla oprávněna zvýšeně monitorovat pohyb svých doručovatelů. Na základě nasbíraných dat navíc dle jejího názoru nebylo možné zaměstnance jasně identifikovat.

Městský soud v Praze však žalobu zamítl a ztotožnil se se stanoviskem ÚOOÚ. Označil *nepřetržité a každodenní sledování každého pohybu zaměstnanců pomocí GPS lokátoru* za nepřiměřený zásah do práva na soukromí, a to z hlediska účelu zpracování. Dále reagoval na shora uvedenou argumentaci České pošty, a.s. tím, že poštovní službu sice lze označit za činnost ve prospěch veřejnosti, ale nejedná se o činnost zvláštní. To, že České poště, a.s. vyplývají povinnosti plnit podmínky licence a zákona, neodůvodňuje narušení soukromí doručovatelů na pracovišti. Tedy při pochůzce na zaměstnavatelem určené trase. Není tedy možné, aby o tyto povinnosti Česká pošta, a.s. opírala neoprávněné zasahování do soukromí svých zaměstnanců.

2. 6 Kamerové systémy

Kamerové systémy jsou audiovizuální či optické prostředky, jimiž dochází k systematickému automatizovanému monitorování konkrétního prostoru.[74] Obklopují nás na každém našem kroku. Jsou umístěné v obchodních střediscích, v blízkosti pozemních komunikací, ale také na pracovištích. Domnívám se, že pokud bychom měli z jednotlivých forem monitoringu vybrat tu formu, která představuje nejintenzivnější zásah do soukromého života zaměstnance, byly by to právě kamerové systémy. Svůj názor zakládám především na skutečnosti, že ze zachycených obrazů lze zpravidla velmi jednoduše sledovanou osobu identifikovat.

[74] Pokyn Evropského sboru pro ochranu osobních údajů č. 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky, verze 2.0. (v originále: *Guidelines 3/2019 on processing of personal data through video devices*) ze dne 29. ledna 2020.

Dle Zahradníčka se nemusí vždy jednat o situaci, kdy bude zaměstnanec rozpoznán dle jeho tváře či jiných zjevných prvků. Zaměstnance může být možné rozpoznat i např. na základě jeho specifické chůze, chování či oblečení.[75] ÚOOÚ říká, že osobní údaj zaměstnance pak představuje souhrn těch identifikátorů, které umožňují propojit osobu se zachyceným jednáním na pořízeném snímku.[76] Na základě těchto důvodů se domnívám, že je žádoucí, aby zaměstnavatel přistupoval k monitoringu prostřednictvím kamerového systému s maximální obezřetností a považoval využití kamerového systému za *ultima ratio* mezi formami monitoringu.

Vodítkem pro určení, kdy bude možné považovat instalaci kamerového systému za oprávněnou, resp. možnou, nám může poskytnout i rozhodovací praxe NSS. Nejvyšší správní soud vydal dne 23. 8. 2013 rozhodnutí, pod sp. zn. 5 As 158/2012, ve kterém zdůrazňuje: „*že k instalaci kamerových systémů, s ohledem na jejich povahu a zásah do osobní integrity osob, je možné přistoupit až tehdy, pokud už veškeré méně invazivní prostředky selhaly anebo by nebyly schopny naplnit vytyčený účel, který je sledován. Je zcela nepochybné, že kamerový systém ve srovnání s jinými prostředky (např. personálními, mechanickými), které mohou dosáhnout naplnění účelů žadatelem sledovanými, zasahuje základní lidská práva, a to právo na soukromí a na soukromý rodinný život, která jsou garantována čl. 10 Listiny základních práv a svobod a v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod, a tudíž i do lidské důstojnosti, z které tato práva vyplývají*.“ V praxi se můžeme setkávat se dvěma základními formami kamerových systémů, a to s kamerovými systémy se záznamovým zařízením a bez záznamového zařízení (tzv. on-line kamery). V minulosti se vycházelo z propozice, dle které docházelo ke zpracování osobních údajů pouze tehdy, bylo-li sledování realizováno kamerovým systémem se záznamovým zařízením. Takové stanovisko bylo zaujímáno např. i ÚOOÚ.[77]

Odchylné stanovisko zaujal Evropský sbor pro ochranu osobních údajů. Evropský sbor pro ochranu osobních údajů uvedl, že i na kamerová zařízení bez záznamu je nutné nahlížet jako na zpracování osobních údajů a postupovat v souladu s GDPR. Stanovil ovšem výjimky, za kterých nebude nutné na

[75] ZAHRADNÍČEK, J. *Ochrana osobnosti v pracovněprávních vztazích*. Praha: Leges, 2019, s. 203. Teoretik. ISBN 978-80-7502-373-5.
[76] ÚOOÚ: Stanovisko č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Leden 2006, s. 1.
[77] Tamtéž.

zpracovávání osobních údajů nahlížet v režimu zpracování osobních údajů dle GDPR. GDPR se nevztahuje např. na zpracování údajů falešnými kamerami či na záznamy kamerových systémů snímaných z výšek, ze kterých nemůže být záznam spojen s konkrétní osobou.[78]

Tento závěr potvrzuje též Nonnemann. Ten nad rámec shora uvedeného zdůrazňuje, že je i v případě kamerových systémů bez zobrazovacího zařízení nutné postupovat v souladu se zásadou proporcionality. Konkrétně to znamená, že bude třeba poměřovat zájem zaměstnavatele vůči zásahu do práva na soukromí zaměstnance.[79]

Zahradníček usuzuje, že by využití monitoringu formou kamerového systému mělo být na pracovišti zaměstnavatelem užito jen v případech předpokládaných v § 316 odst. 2 ZP. Ve smyslu § 316 odst. 1 ZP totiž dle jeho názoru nebude možné označit monitoring kamerovým systémem za přiměřený způsob kontroly.[80] Shodné stanovisko jako Zahradníček zastává též Státní úřad inspekce práce.[81]

Pracovní skupina WP29 pak uvádí, že z namátkových kontrol, které byly provedeny, vyplývají především následující účely, pro které jsou kamerové systémy zaváděny. Jsou jimi: *ochrana jednotlivců*, *ochrana majetku*, *veřejný zájem*, *odhalování, prevence* a *stíhání trestné činnosti* či *získávání důkazů.*[82]

Pro zavedení monitoringu kamerovým systémem bude tedy také nezbytné, aby byl naplněn závažný důvod spočívající ve zvláštní činnosti zaměstnavatele. Dle Pejchalové Grünwaldové mají být *mutatis mutandis* aplikovány při zavádění monitoringu kamerovým systémem principy, které byly založeny v rozhodnutí Evropského soudu pro lidská práva ze dne 5. září 2017 ve věci 61496/08 –

[78] Bod 8 Pokynu 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky, verze 2.0. (v originále: *Guidelines 3/2019 on processing of personal data through video devices*) ze dne 29. ledna 2020.
[79] NONNEMANN, F. Vztahuje se GDPR i na online kamery?. *Epravo.cz.* [online]. Publikováno 2. 3. 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/vztahuje-se-gdpr-i-na-online-kamery-110746.html.
[80] ZAHRADNÍČEK, J. *Ochrana osobnosti v pracovněprávních vztazích*. Praha: Leges, 2019, s. 204. Teoretik. ISBN 978-80-7502-373-5.
[81] Státní úřad inspekce práce. *Monitorování zaměstnanců na pracovišti kamerovým systémem. Otázky a odpovědi*. [online]. Publikováno 7. 4. 2014 [cit. 31. 3. 2022]. Dostupné z: http://www.suip.cz/otazky-a-odpovedi/pracovnepravni-vztahy/ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance/monitorovani-zamestnancu-na-pracovisti-kamerovym-systemem-pridano-7-14-2014/.
[82] Pracovní skupina zřízená dle čl. 29 Směrnice 95/46/ES: Stanovisko č. 4/2004 – Ke zpracování osobních údajů prostředky kamerového sledování (11750/02/EN/WP89) (v originále: *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*) ze dne 11. února 2004, s. 3, dostupné na: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf.

Bărbulescu proti Rumunsku.[83] Přestože se domnívám, že ochrana vlastnického práva bude uváděna jako nejčastější důvod pro zavedení tohoto monitoringu, myslím si, že jako důvod může být akceptována též ochrana bezpečnosti a zdraví zaměstnanců.

Pojmem *zvláštní činnost* se pak zabýval např. Městský soud, který za takovou označil „*nakládání s vysoce nebezpečnými chemikáliemi či s vysokými finančními příklady.*“[84] Tyto pojmy se vztahují například na zaměstnance čerpacích stanic či kurýry převážející ceniny. Naopak důvod, pro který by zaměstnavatel dle stanoviska Evropského sboru pro ochranu osobních údajů zavádět kamerový systém neměl, je monitoring výkonnosti zaměstnanců či objemu jimi odvedené práce. Dle mého názoru si však lze představit kupříkladu i situaci, kdy zaměstnavatel bude instalovat kamerové systémy na pracovišti za účelem prevence trestné činnosti. Například ve vojenském průmyslu, kde prozrazení technických *know how* může mít nepříjemné důsledky v eventuálním vojenském sporu. Dalším příkladem, který lze uvést je opět kurýr převážející ceniny. Jedná se o profesi, u které může mít zaměstnavatel důvodnou obavu z toho, aby nedošlo ke zcizení těchto cenin.

2. 6. 1 Rozsudek Městského soudu v Praze ze dne 18. 10. 2016, sp. zn. 5 A 107/2013

Také u monitoringu zaměstnanců prostřednictvím kamerového systému bude nutné naplnit zásadu subsidiarity a proporcionality. Jako příklad nám může posloužit výše uvedené rozhodnutí Městského soudu v Praze. V tomto rozhodnutí Městský soud v Praze řešil případ monitoringu řidičů významného českého dopravního přepravce (Student Agency s.r.o.).

Ten zavedl monitoring za účelem ochrany majetku (především autobusů), zdraví zaměstnanců, zvýšení bezpečnosti přepravy cestujících, ale i za účelem zajištění důkazního materiálu při potenciálně vzniknuvších dopravních nehodách. Dalším argumentem bylo také případné projednávání stížností od přepravovaných cestujících. Dle zaměstnavatele navíc představuje provozování autobusové dopravy (vnitrostátní i mezinárodní linky) zvláštní činnost, neboť se jedná o činnost

[83] PEJCHALOVÁ GRÜNWALDOVÁ, V. Evropský soud pro lidská práva: K zásahu do soukromí zaměstnanců. *Advokátní deník.* [online]. Publikováno 19. 3. 2020 [cit. 31. 3. 2022]. Dostupné z: https://advokatnidenik.cz/2020/03/19/evropsky-soud-pro-lidska-prava-k-zasahu-do-soukromi-zamestnancu.

[84] Rozsudek Městského soudu v Praze ze dne 18. 10. 2016, sp. zn. 5 A 107/2013.

nebezpečnou. Student Agency s.r.o se domnívá, že při provozování dopravních služeb potenciálně hrozí vyšší míra vzniku dopravních nehod. V jejich důsledku pak mohou vznikat majetkové škody různého rozsahu či ztráty na životech, a to jak zaměstnanců, tak cestujících (jeden autobus převeze cca 64 cestujících).

Jak jsem již zmínila výše, na tomto případě lze prezentovat též zásadu subsidiarity a proporcionality. Soud zde dospěl k závěru, že v daném případě bylo fakticky nemožné společností Student Agency s.r.o. naplnit stanovené účely. Argumentoval tím, že monitorováním kabiny řidičů nelze přispět k ochraně zdraví a bezpečnosti cestujících. Kamera namířená na řidiče zase nemůže předcházet dopravní nehodě. V tomto případě by větší smysl dávala kamera snímající okolí před autobusem. Jako důkazní materiál navíc může posloužit svědectví cestujících. Ti mohou také mj. nejlépe poskytnout zaměstnavateli zpětnou vazbu o kvalitě jím poskytovaných služeb. V daném případě soud prováděl tzv. test proporcionality. Posuzoval v něm kolizi mezi právem na ochranu majetku, právem na ochranu života a zdraví zaměstnanců a cestujících a právem zaměstnanců (jak řidičů, tak stewardů) na ochranu jejich soukromí na pracovišti.

Soud zde dospěl k názoru, že k naplnění principu proporcionality nedošlo. Účelu totiž mohl zaměstnavatel dosáhnout i jinými, méně invazivními zásahy do soukromí zaměstnanců. Dodržování pravidel silničního provozu si mohl zaměstnavatel kupř. ověřit záznamem již z jiných kamer, které byly na kapotě autobusů nainstalovány z důvodu zajištění bezpečnosti. Zaměstnavatel navíc mohl provádět i namátkové kontroly. Ty jsou méně invazivním zásahem do soukromí zaměstnanců. O tom, že jsou namátkové kontroly naplánovány, by zaměstnanci věděli. Nebyli by však srozuměni s tím, na jaké konkrétní lince bude namátková kontrola realizována. Osoby, které by kontrolu prováděly, by pak po praktické stránce plnily shodnou preventivní funkci jako kamery.

Závěrem soud upozornil, že v tomto konkrétním případě nebylo *de facto* zachováno ani minimální právo zaměstnance na soukromí. Řidiči autobusů jsou po celou pracovní dobu na jednom místě, a to za volantem na místě řidiče. Podléhali proto téměř nepřetržitému monitoringu. Systematický a nepřetržitý monitoring je intenzivním a nepřiměřeným zásahem do práva zaměstnance na jeho soukromý život.[85] Požadavek proporcionality tedy nebyl naplněn.

[85] Rozsudek ESLP ze dne 25. září 2001, P. G. a J. H. proti Spojenému království, č. stížnosti 44787/98.

2. 6. 2 Rozsudek ve věci č. 1874/13 a 8567/13 Lopéz Ribalda a ostatní proti Španělsku

Na úrovni ESLP lze označit za jedno z nejvýznamnějších rozhodnutí, rozhodnutí ve věci Lopéz Ribalda a ostatní proti Španělsku. V daném případě ESLP rozhodoval o stížnosti zaměstnanců, kteří byli zaměstnáni v obchodním řetězci. Vzhledem k tomu, že se v inventurách objevovaly velké nesrovnalosti, nainstaloval zaměstnavatel do prostor obchodního řetězce kamerový systém. Některé kamery byly skryté, jiné viditelné. O tom, že byly některé kamery nainstalovány u vchodu obchodu, byli zaměstnanci zaměstnavatelem informováni. Nedisponovali však již informací o tom, že některé kamery jsou nainstalovány též v blízkosti pokladen.

Výsledkem tohoto tajného sledování pokladen prostřednictvím kamerového systému bylo zjištění, že někteří zaměstnanci ve spolupráci se třetími osobami opravdu kradli. Tito zaměstnanci byli na základě tohoto zjištění propuštěni. S tím se však zaměstnanci nesmířili a platnost výpovědi napadali jak u soudu prvního, tak druhého stupně. Bezúspěšně. Stěžovatelé se proto obrátili se svou stížností na ESLP. Namítali, že provedením důkazu záznamem z kamerového systému namířeného na pokladnu, bylo porušeno jejich právo na soukromí (čl. 8 Úmluvy). Argumentovali tím, že nebyli zaměstnavatelem informováni o tom, že jsou kamery namířeny též na pokladny. Dle vnitrostátního práva Španělského království musí být o instalaci videokamer na pracovišti zaměstnavatelem informováni všichni zaměstnanci. Informační povinnost však v tomto případě zaměstnavatel nesplnil. Kamerovým systémem zaměstnavatel navíc snímal všechny zaměstnance, nikoliv pouze ty, u nichž měl důvodné podezření, že kradou. Senátem ESLP soud rozhodl tak, že došlo k porušení čl. 8 Úmluvy, protože vnitrostátní soudy nesprávně nalezly a posoudily rovnováhu mezi právem zaměstnance na soukromí a ochranu vlastnického práva zaměstnavatele. Zaměstnavatel navíc překročil vnitrostátní úpravu tím, že nesplnil svou informační povinnost.

Odlišně se však k dané problematice postavil velký senát ESLP. Ten konstatoval, že je pravdou, že nesplněním informační povinnosti došlo ze strany zaměstnavatele k porušení vnitrostátní právní úpravy. Zaměstnavatel měl své zaměstnance informovat též o instalaci kamer nad pokladnami. ESLP avšak také konstatoval, že vnitrostátní soudy dostatečně posoudily další okolnosti, tj. veřejný charakter sledovaného prostoru (jednalo se o obchodní centrum, které bylo

přístupné veřejnosti), délku trvání záznamu (sledování nebylo dlouhodobé), jeho zpracování (záznam z kamer byl použit výhradně k prošetření ztráty zboží a nesrovnalostí v inventuře) aj.

Za zohlednění všech shora uvedených okolností proto mohly vnitrostátní soudy dospět k názoru, že zásah do soukromí zaměstnance byl zásahem přiměřeným. K porušení čl. 8 Úmluvy tedy nedošlo. Zaměstnanci byli ESLP odkázáni na uplatnění náhrady škody. Mimo jiné ESLP uvedl, že zaměstnavatel byl v daném případě ohrožen nikoliv pouze potenciálním jednáním jednoho zaměstnance, ale jednáním větší skupiny zaměstnanců. U těchto zaměstnanců se mohl důvodně obávat, že páchají soustavnou trestnou činnost ve větším rozsahu.

2. 7 Elektronické docházkové systémy

Další formu monitoringu představují elektronické docházkové systémy. Do těchto elektronických docházkových systémů zaměstnanec zanáší svůj příchod a odchod, přestávku na oběd, odpočinek, ale též např. odchod k lékaři. Z docházkového systému musí vyplývat údaje o práci přesčas, noční práci a též odpracované pracovní době.[86] Zaměstnavatelé prostřednictvím zavádění elektronických docházkových systémů splňují svou povinnost stanovenou jim v ust. § 96 ZP. Zaměstnavatelé dle tohoto ustanovení musí vést evidenci u jednotlivých zaměstnanců. To, jakou formu evidence pracovní doby by měl zaměstnavatel využít, dále zákoník práce nerozvádí. Dle Uhrinové se proto zpravidla bude jednat o monitoring oprávněný a odpovídající svému účelu.[87]

Odlišná situace by mohla nastat tehdy, bylo-li by u elektronického docházkového systému využíváno biometrických údajů. „*Biometrickými údaji se rozumí osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují nebo potvrzují jejich jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.*“[88] GDPR zakazuje zpracování biometrických údajů

[86] ŠTEFKO, M. In: BĚLINA, M., DRÁPAL, L. a kol. *Zákoník práce*. 3. vydání. Praha: C. H. Beck, 2019, s. 520, marg. č. 1. § 96 [Evidence pracovní doby].
[87] UHRINOVÁ, A., MENZELOVÁ K. *Vybrané způsoby monitoringu zaměstnance pracujícího z domova a jejich právní mantinely.* In.: MORÁVEK J. (ed.). *Pracovní právo 2021: Sociální právo v době (post)covidové*. 1. vydání. Praha: Univerzita Karlova, Právnická fakulta, 2021. s. 85-105. ISBN: 978-80-7630-016-3. Online dostupné z: https://rozkotova.cld.bz/Pracovni-pravo-2021?fbclid=IwAR1kY.
[88] Úřad pro ochranu osobních údajů. Připomínka k návrhu zákona, kterým se mění zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů a zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, s. 2. Dostupné zde: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=35418.

zpracovávaných za účelem jedinečné identifikace fyzické osoby (čl. 9 odst. 1 GDPR). Z daného důvodu někteří odborníci odvozují, že bude-li nastaven docházkový systém například tak, že zaměstnanec nejdříve zadá do elektronického docházkového systému své zaměstnavatelem přiřazené osobní číslo, jméno či např. přidělený pin (tedy provede svou identifikaci) a následně přiloží svůj otisk prstu, bude možné docházkový systém s biometrickými údaji využít.[89] V tomto případě totiž nebude otisk prstu sloužit k identifikaci, ale pouze k ověření toho, že se jedná o konkrétní osobu zaměstnance.

Domnívám se, že takto vybavené elektronické docházkové systémy by zaměstnavatel mohl oprávněně užít u zaměstnanců pracujících ve výzkumných laboratořích. Ve výzkumných laboratořích se často pracuje jak s látkami drahými, tak s látkami nebezpečnými. Některé státy investují do svých výzkumných laboratoří značné finanční prostředky. Příkladem může být vojenský výzkum biologických zbraní. Pandemie onemocnění Covid-19 však ukázala též to, jak významný je výzkum ve zdravotnictví. Farmaceutické společnosti se předháněly v tom, která z nich uspěje na trhu a vyvine jako první účinnou vakcínu proti onemocnění Covid-19. Byla-li bych vlastníkem takových farmaceutických společností, zajisté by bylo mým zájmem zamezit přístupu neoprávněných osob do mé laboratoře. Mé obavy by mohly pramenit z toho, že dojde k prozrazení *know how*, postupů, ale také z možného úniku nebezpečných látek.

2. 8 Povinné testování zaměstnanců na přítomnost viru SARS-CoV-2 (tzv. covid-19)

V důsledku pandemie onemocnění covid-19 jsme se v posledních měsících setkávali s novou formou monitoringu. Tato forma spočívala v antigenním testování zaměstnanců na přítomnost viru SARS-CoV-2. Testování zaměstnanců bylo zásahem do práva na informační sebeurčení zaměstnanců.[90] Zaměstnavatelům byla tato povinnost uložena mimořádnými opatřeními Ministerstva zdravotnictví.[91] Za nejvýznamnější z těchto opatření bych označila mimořádné opatření Ministerstva zdravotnictví ze dne 1. března 2021, č. j. MZDR 47828/2020-

[89] LUPIENSKÁ, P. Docházkový systém s použitím biometriky - otisk prstů zaměstnanců. Co na to GDPR?. *Právní prostor.* [online]. Publikováno 17. 3. 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.pravniprostor.cz/clanky/spravni-pravo/dochazkovy-system-s-pouzitim-biometriky-otisky-prstu-zamestnancu-co-na-to-gdpr?.
[90] Bod 84 Rozsudku Nejvyššího správního soudu ze dne 14. dubna 2021, sp. zn. 8 Ao 1/2021.
[91] Např. mimořádné opatření Ministerstva zdravotnictví MZDR 47828/2020-16/MIN/KAN, MZDR 47828/2020-22/MIN/KAN či MZDR 9364/2021-1/MIN/KAN.

16/MIN/KAN[92] (dále také jako „opatření“). Zaměstnavateli vyplynuly z tohoto opatření tři důležité povinnosti. Zaměstnavatel měl povinnost umožnit osobní přítomnost na pracovišti pouze těm zaměstnancům, kteří podstoupili v rozhodném období test[93] s výsledkem negativní. Zaměstnavatel měl dále povinnost vyzvat své zaměstnance k tomu, aby tyto testy absolvovaly a zajistit možnost takového testování. ÚOOÚ předložil zaměstnavatelům dva způsoby, jakým mohla být povinnost zajištění testů splněna.[94] První způsob spočíval ve využití poskytovatelů zdravotních služeb. Tomuto způsobu se v této diplomové práci nebudu blíže věnovat. Práce je totiž obsahem zaměřena na monitoring, který je zaměstnavateli prováděn přímo, nikoliv zprostředkovaně. Z tohoto důvodu budu dále svou pozornost věnovat druhé ze stanovených forem. Ta spočívá v testování zaměstnanců samotným zaměstnavatelem.

U takového testování zaměstnavatel vystupuje jako správce údajů dle GDPR či ZOOÚ, protože zpracovává údaj o zdravotním stavu[95]. Ten se v souladu se článkem 9 GDPR řadí do zvláštní kategorie osobních údajů. Aby mohl být údaj o zdravotním stavu dle článku 9 GDPR zpracováván, musí být naplněn některý z důvodu uvedených v odstavci 2 tohoto článku. V případě testování zaměstnanců byl zaměstnavatel během pandemie onemocnění covid-19 oprávněn tyto údaje zpracovávat, neboť v tomto konkrétním případě bylo zpracování o zdravotním stavu zaměstnanců nezbytné pro účely plnění povinností a výkon zvláštních práv správce údajů v oblasti pracovního práva (čl. 9. odst. 2 písm. b) GDPR). Zaměstnavatelé měli vést pro kontrolní účely evidenci provedených testů. Otázkou zůstává, zda může zaměstnavatel své zaměstnance testovat, a tím monitorovat jejich zdravotní stav i nyní, kdy mu tato povinnost ze žádného nařízení či právního předpisu nevyplývá a onemocnění covid-19 je na ústupu? Názory se různí.

Dle Odrobinové může zaměstnavatel v testování zaměstnanců stále pokračovat. Odkazuje přitom na § 102 ZP. Zaměstnavatel je dle tohoto ustanovení povinen vytvářet bezpečné a zdraví neohrožující pracovní prostředí. Odrobinová

[92] Ministerstvo zdravotnictví České republiky. *Mimořádné opatření*. [online]. Publikováno 1. 3. 2020. [cit. 31. 3. 2022] Dostupné z: https://www.mzcr.cz/wp-content/uploads/2021/03/Mimoradne-opatreni-povinne-testovani-zamestnavatele-s-ucinnosti-od-3-3-2021-do-odvolani.pdf.
[93] RT-PCR test na přítomnost viru SARS-CoV-2, antigenní test na přítomnost antigenu viru SARS-CoV-2.
[94] Úřad pro ochranu osobních údajů. *K povinnému testování zaměstnanců – rozšířené vyjádření.* [online]. Změněno 26. 3. 2021. [cit. 31. 3. 2022] Dostupné z: https://www.uoou.cz/k-povinnemu-testovani-zamestnancu-rozsirene-vyjadreni/d-48835.
[95] Dle bodu 35 jsou mezi údaje o zdravotním stavu zahrnuty též informace získané během provádění testů, tj. též testů antigenních.

proto dospívá k závěru, že zaměstnavatel může přijmout opatření proti šíření onemocnění covid-19. Opatření však musí přijímat s cílem zajištění bezpečnosti a zdraví svých zaměstnanců. Zdůrazňuje, že na pracovněprávní vztah je i v tomto případě nutno nahlížet jako na vztah nerovný, ve kterém má zaměstnanec slabší postavení. V případě, kdy se zaměstnavatel pro toto opatření rozhodne, měl by v první řadě vyhodnotit epidemiologické riziko. Potřebnost takového opatření bude odlišná v době stagnace pandemie a v době její expanze. Například nyní se šíření onemocnění covid-19 zpomaluje. Dále by zaměstnavatel měl vždy zvážit, zda nemohou být využity méně invazivní způsoby zásahu do soukromí zaměstnance.[96] Můj zaměstnavatel například nainstaloval u vchodu na pracoviště elektronické zařízení, které měřilo všem příchozím zaměstnancům teplotu. Tím eliminoval pohyb osob s vysokou teplotou (jako jedním z příznaků onemocnění covid-19) po pracovišti, aniž by intenzivně zasahoval do práva na soukromí. Věřím, že instalace takových zařízení může být užitečná při šíření jakéhokoliv onemocnění, u kterých je teplota typickým symptomem.

K opačnému závěru dospívá Vališová. Dle jejího názoru není možné nahlížet na ustanovení § 102 odst. 1 ZP jako na povinnost zaměstnavatele k tomu, aby převzal odpovědnost za celkový zdravotní stav svých zaměstnanců. V situaci, kdy by zaměstnavatel chtěl převzít odpovědnost za celkový zdravotní stav svých zaměstnanců a tím zajistit bezinfekčnost pracovního prostředí, by musel své zaměstnance testovat pravidelně, a to na všechna infekční onemocnění. Covid-19 totiž není jediným infekčním onemocněním, se kterým se na pracovišti můžeme setkat. Vanišová shrnuje, že požadavky zaměstnavatele musí být oprávněné a ospravedlnitelné.[97]

Můj názor k této problematice je takový, že zaměstnavatel by měl mít zájem na zajištění, co možná nejlepších pracovních podmínek, tj. prostředí bezinfekčního a zdraví neškodlivého. Ačkoliv se odborné názory na šíření onemocnění covid-19 na pracovišti též rozcházejí, myslím si, že v době největšího růstu pandemie bylo testování oprávněné. Především u infekčních variant, které se rychle šíří. Souhlasím však též se závěrem Vališové, že onemocnění covid-19 není jediným infekčním

[96] ODROBINOVÁ, V. Nařízené testování zaměstnanců z pohledu GDPR. *Práce a mzda.* [online]. Publikováno 22. 10. 2021. [cit. 31. 3. 2022]. Dostupné z:https://www.praceamzda.cz/clanky/narizene-testovani-zamestnancu-z-pohledu-gdpr.

[97] VALIŠOVÁ, V. K otázce interních předpisů zaměstnavatele ve vztahu k prevenci onemocnění covid-19 v otázkách a odpovědích. *Advokátní deník.* [online]. Publikováno 10. 9. 2021. [cit. 31. 3. 2022]. Dostupné z: https://advokatnidenik.cz/2021/09/10/k-otazce-internich-predpisu-zamestnavatele-ve-vztahu-k-prevenci-onemocneni-covid-19-v-otazkach-a-odpovedich/.

onemocněním. Šíření infekčních nemocí nepřispívá ani současná situace související s migrací a uprchlickou krizí. S ohledem na situaci na Ukrajině bude s vysokou pravděpodobností do budoucna narůstat počet nakažených osob. Dle mého názoru se budeme v budoucnu setkávat i s dalšími infekčními onemocněními, například se žloutenkou, černým kašlem, tuberkulózou či dalšími variantami covidu. Povinné očkování totiž není napříč státy jednotné. V případě, že zaměstnavatel dokáže dostatečně odůvodnit potřebu takového opatření či nabídne svým zaměstnancům jiné, méně invazivní metody (např. práci z domova), nemyslím si, že by bylo jeho jednání protiprávní.

2. 8. 1 Rozsudek NSS ze dne 4. března 2022, sp. zn. 5 Ao 31/2021

Závěrem bych ráda uvedla, že mým cílem v této kapitole nebylo hodnotit právní korektnost předmětného opatření. Dovolím si však čtenáře odkázat na v tomto kontextu velice významný rozsudek Nejvyššího správního soudu ze dne 4. března 2022, sp. zn. 5 Ao 31/2021 (dále také *„rozsudek“*). Tímto rozsudkem NSS zamítl návrh na zrušení mimořádného opatření Ministerstva zdravotnictví ze dne 20. listopadu 2021, č. j. MZDR 42085/2021-1/MIN/KAN ve znění mimořádného opatření Ministerstva zdravotnictví č. j. MZDR 42085/2021-2/MIN/KAN[98]. Toto mimořádné opatření ukládalo zaměstnavatelům povinnost testovat své zaměstnance jednou za sedm dnů. Výjimku z testování měli zaměstnanci s dokončeným očkováním a ti, kteří prodělali laboratorně potvrzené onemocnění covid-19. Zaměstnanci, kteří nesplňovali podmínku a odmítli se testovat, museli na pracovišti dodržovat odstup, odděleně se stravovat a nosit ochranný prostředek dýchacích cest. Zaměstnavatel měl povinnost organizačním opatřením omezit setkávání těchto zaměstnanců s jinými zaměstnanci či osobami na nezbytnou míru. Navrhovatel shledával, že opatření zasahuje do pracovně právního vztahu mezi zaměstnavatelem a zaměstnanci, tím, že jim ukládá povinnosti nad rámec zákoníku práce či souvisejících právních předpisů (bod 4 rozsudku).

NSS v bodu 37 tohoto rozsudku stanovil, že účelem Ministerstvem zdravotnictví přijímaných opatření je ochrana veřejného zdraví, resp. ochrana společnosti před šířením onemocnění covid-19. Jedním z nástrojů pro naplnění

[98] Ministerstvo zdravotnictví České republiky. *Mimořádné opatření*. [online]. Publikováno 22. 11. 2020. [cit. 31. 3. 2022] Dostupné z: https://www.mzcr.cz/wp-content/uploads/2021/11/Zmena-mimoradneho-opatreni-ze-dne-20-11-2021-k-testovani-zamestnancu-a-osob-samostatne-vydelecne-cinnych-s-ucinnosti-od-23-11-2021.pdf.

tohoto účelu je plošné testování zaměstnanců. Účelu bude moci být však dosaženo pouze tehdy, pokud se do povinného testování zapojí co nejvíce osob. Ministerstvo zdravotnictví se při přijímání opatření snaží o co nejmenší omezení společnosti. Musí však vždy upřednostňovat ochranu života a zdraví občanů. Na pravidelné testování zaměstnanců je tak třeba nahlížet jako na kompromis. V tomto kompromisu je na jedné straně nezbytnost zamezení šíření onemocnění covid-19 a na straně druhé ekonomické aspekty, ochrana před uzavíráním podniků či nedostatek zdravotnického personálu (bod 75 rozsudku). NSS návrh odmítl, s tím, že opatření sleduje legitimní cíl, kterého lze preventivním testováním dosáhnout (79 rozsudku). Tímto cílem je ochrana života a zdraví občanů České republiky.

3 Povinnosti zaměstnavatele ve vztahu k monitoringu

Pouhé vyhodnocení, že je monitoring či kontrola zaměstnance dle zákoníku práce oprávněný, není dostačující. Zaměstnavatel je povinen vždy vyhodnotit, jaké požadavky jsou na něj kladeny. Jak bylo nastíněno v první kapitole diplomové práce, monitoring zaměstnanců totiž není upraven pouze zákoníkem práce. Zaměstnavatel musí při každé prováděné kontrole či monitoringu zaměstnanců splňovat jak požadavky kladené zákoníkem práce, tak požadavky kladené jinými právními předpisy. Především požadavky vyplývající z GPDR, neboť při monitoringu a kontrole zaměstnance pravidelně dochází ke zpracovávání osobních údajů.[99]

Každý z těchto předpisů ukládá zaměstnavatelům jiné povinnosti. Vzhledem k omezenému rozsahu diplomové práce se nelze všemi zaměstnavatelům uloženými povinnostmi podrobně zabývat. Z tohoto důvodu jsem se při vytváření obsahu této kapitoly inspirovala v relevantní judikatuře českých soudů a Evropského soudu pro lidská práva. Věnována je pozornost především těm povinnostem, jejichž nesplnění či nesprávná interpretace jsou zaměstnavatelům nejčastěji těmito soudy vytýkány. S ohledem na vzrůstající vliv nadnárodních korporací upravuje část této kapitoly také přeshraniční předávání osobních údajů našich zaměstnavatelů do zahraničí.

3. 1 Zásada proporcionality

Zásadu proporcionality lze charakterizovat jako zásadu, dle které mají být v průběhu monitoringu oprávnění zaměstnance v souladu s legitimními oprávněními a zájmy zaměstnavatele.[100] V pracovněprávním vztahu zaměstnanec přiměřeně předpokládá zachování práva na jeho soukromí. Zaměstnavatel naopak od zaměstnance oprávněně očekává, že bude zaměstnanec využívat pracovní dobu k plnění pracovních úkolů. Zaměstnavatel dále vyvíjí oprávněně úsilí pro ochranu svých statků a požaduje po zaměstnancích, aby soukromé záležitosti v pracovní době vyřizovali jen v nezbytném a přiměřeném rozsahu.[101] V rámci monitoringu

[99]UHRINOVÁ, A., MENZELOVÁ K. *Vybrané způsoby monitoringu zaměstnance pracujícího z domova a jejich právní mantinely.* In.: MORÁVEK J. (ed.). *Pracovní právo 2021: Sociální právo v době (post)covidové*. 1. vydání. Praha: Univerzita Karlova, Právnická fakulta, 2021. s. 85-105. ISBN: 978-80-7630-016-3. Online dostupné z: https://rozkotova.cld.bz/Pracovni-pravo-2021?fbclid=IwAR1kY.

[100] VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců*. V Praze: C. H. Beck, 2013, s. 104. Beckova edice ABC. ISBN 978-80-7400-453-7.

[101] KADLECOVÁ, T. GPS ve služebních vozidlech aneb malý čip = velká komplikace?. *Praktická personalistika*. Sagit, 2015, 2015(3-4/2015).

zaměstnanců se bude jednat především o posuzování konfliktu dvou základních práv garantovaných Listinou, a to práva na ochranu soukromí (č. 7 odst. 1 Listiny, čl. 10 Listiny) a práva na ochranu života a majetku (čl. 6 odst. 1 Listiny a čl. 11 odst. 1 Listiny).[102] Před zavedením jakéhokoliv konkrétního monitoringu by měl zaměstnavatel posoudit, zda přínosy tohoto monitoringu převáží nad nepříznivým dopadem na právo na soukromí dotčeného zaměstnance, jakož i na práva třetích osob.[103] Kupř. monitoring e-mailové adresy se totiž nedotýká pouze práva na soukromí konkrétních zaměstnanců, ale též práva třetích osob, které se zaměstnanci komunikují.

Podmínky omezování základních práv a svobod garantovaných Listinou stanovuje judikatura Ústavního soudu. Ústavní soud vymezil tzv. test proporcionality, ve kterém uvádí tři kritéria. Prvním kritérium, kterým se zabývá, je vhodnost. Dle kritéria vhodnosti se dle Ústavního soudu posuzuje, zda institut, který omezuje určité základní právo, umožní dosáhnout sledovaného cíle. Zda se kupř. opravdu zavedením kamerových systémů na pracovišti, které představují významný zásah do práva na soukromí zaměstnance, dosáhne zamezení krádeží zaměstnanci na prodejně. Druhým kritériem je kritérium potřebnosti. To spočívá v porovnávání legislativního prostředku, který omezuje základní právo či svobodu, s jiným opatřením, které umožňuje dosáhnout stejného cíle bez toho, aby se dotkl základních práv či svobod. Jako příklad uvádím situaci, která nenaplňuje charakteristiky potřebnosti. Jedná se o případ, kdy zaměstnavatel umístí do svých firemních vozů GPS lokátory a jako důvod uvede kontrolu, zda zaměstnanci vozidla neužívají k jiným než stanoveným účelům. Zde si myslím, že by soud mohl porovnávat, zda stejného účelu nedosáhne zaměstnavatel kupř. řádnou kontrolou knih jízd. Dle třetího kritéria testu proporcionality se pak porovnává závažnost obou v kolizi stojících základních práv. U monitoringu to bude velmi často v kolizi právo vlastnické s právem na soukromí.[104]

Zásadou proporcionality se zabýval i Evropský soud pro lidská práva, a to ve svém rozhodnutí ze dne 5. září 2017, Bărbulescu proti Rumunsku, číslo stížnosti 61496/08. Evropský soud pro lidská práva v tomto případě řešil monitoring zaměstnanců prostřednictvím kamerového systému. Ačkoliv zásady ESLP v tomto

[102] Rozsudek Nejvyššího správního soudu ze dne 20. 12. 2017, sp. zn. 10 As 245/2016.
[103] Rozsudek Evropského soudu pro lidská práva ze dne 12. ledna 2016, stížnost č. 61496/08, BĂRBULESCU proti Rumunsku, str. 26.
[104] Nález Ústavního soudu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94.

rozhodnutí vyslovené byly stanoveny za účelem poměřování naplnění proporcionality vnitrostátními soudy, domnívám se, že je vhodné, aby si tyto zásady před zavedením jednotlivých forem monitoringu vyhodnotil každý zaměstnavatel. Každá z forem monitoringu je totiž zásahem do soukromí, ať už méně či více invazivním. Zájem zaměstnavatele nebude převažovat vždy nad právem na ochranu soukromí zaměstnance. Dospívám proto k závěru, že pokud si zaměstnavatel takovéto hodnocení samostatně provede, minimalizuje tím možnost soudního sporu či zhoršení vztahů se zaměstnanci.

Odmyslíme-li informační povinnost, které je věnována samostatná část této kapitoly, měl by zaměstnavatel primárně zvažovat rozsah monitoringu. Zaměstnavatel by se měl zamyslet nad otázkou, zda bude zaváděn monitoring dlouhodobý, nebo monitoring časově omezený (například v řádu několika dnů). Dále by se měl zabývat tím, zda bude monitoring zaměřen na všechny zaměstnance či pouze na konkrétní jednotlivce. Kromě toho by měl zaměstnavatel zvážit, zda mu svědčí legitimní důvod pro konkrétní formy monitoringu. Zaměstnavatel by měl závěrem dostatečně posuzovat též důsledky, které bude mít monitoring pro konkrétního zaměstnance. Má-li být vysloven soulad monitoringu se zásadou proporcionality, je nutné, aby ochrana hodnoty, pro kterou je monitoring zaváděn, zasluhoval vyšší míru ochrany než právo zaměstnanců na zachování soukromí. Takovou hodnotou může být například život či zdraví zaměstnance.

3. 2 Princip minimalizace údajů

Zaměstnavatel je při monitoringu, v jehož důsledku dochází ke zpracovávání osobních údajů, povinen dodržovat princip minimalizace údajů. Zpracovávané údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (čl. 5 odst. 1 GDPR). Zaměstnavatel smí zpracovávat pouze ty údaje, které jsou pro konkrétní účel nezbytné. Zaměstnavatel naopak nesmí zpracovávat a shromažďovat údaje, které s jím vytyčeným účelem vůbec nesouvisí nebo souvisí pouze okrajově. Shromažďovat a dále zpracovávat nesmí ani údaje, které nejsou pro dosažení účelu důležité.[105] Údaje v rámci monitoringu mají být zpracovávány v nezbytném rozsahu pro naplnění konkrétního účelu. Domnívám se, že je proto žádoucí, aby si zaměstnavatel vymezil tento účel ještě před tím, než monitoring na pracovišti

[105] RÁMIŠ, V. In: UŘIČAŘ, M., RÁMIŠ, V. a kol. *Obecné nařízení o ochraně osobních údajů.* 1. vydání. Praha: C. H. Beck, 2021, s. 303, marg. č. 94. Článek 5 [Zásady zpracování osobních údajů].

zavede. Tento účel musí být vždy v souladu se zákonem. Je proto nepřípustné, aby si zaměstnavatel za účel stanovil kupříkladu šikanu svých zaměstnanců či jejich diskriminaci. Využije-li naopak zaměstnavatel svého oprávnění dle § 316 odst. 1 ZP a zavede monitoring za účelem kontroly dodržování zákazu využívání svěřených prostředků, bude účel monitoringu legitimní.

3. 3 Informační povinnost

Zaměstnavatel je povinen zaměstnance informovat o důvodech a formě monitoringu. O tom, jaké metody a techniky bude při zpracování údajů užívat a též o tom, jak dlouhou dobu bude monitoring probíhat.[106] Zaměstnavatel je povinen před uzavřením smlouvy seznámit zaměstnance s právy a povinnostmi, které mu vyplývají z pracovní smlouvy či pracovními podmínkami, za nichž zaměstnanci mají práci pro zaměstnavatele konat. Zaměstnavatel je dále povinen seznámit zaměstnance s povinnostmi, které mu vyplývají ze zvláštních právních předpisů vztahujících se k práci, která má být předmětem pracovního poměru (§ 31 ZP). V případě, kdy je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze jeho činnosti, který odůvodňuje zavedení kontrolních mechanismů podle § 316 odst. 2 ZP, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a způsobech jejího provádění (§ 316 odst. 3 ZP). Takovou činností je například činnost s ceninami.

Informační povinnost zaměstnavatel musí splnit také vůči GDPR. Pro zaměstnavatele je klíčový především článek 13 GDPR. Zaměstnavatel má povinnost poskytnout zaměstnanci v okamžiku získání osobních údajů informace o zaměstnavateli. Těmito informacemi jsou jeho kontaktní údaje a kontaktní údaje na pověřence pro ochranu osobních údajů, pokud je zřízen. Dále je povinen seznámit zaměstnance s účely, pro které konkrétní osobní údaje zaměstnance slouží, a na jakém právním základě budou zpracovávány. Právní základ charakterizuje ÚOOÚ jako právem předpokládaný důvod zpracování, kterým disponuje jak zpracovatel, tak správce.[107] Zaměstnanci náleží právo být pravidelně informován o osobních údajích, které o něm zaměstnavatel uchovává. Dále má

[106] International Labour Office (ILO). *Code of Practice: Protection of Worker's personal data*.). Geneva: International Labour Office, 1997. Čl. 6.14. a násl. ISBN 92-2-110329-3. Online dostupný z: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf.

[107] Úřad pro ochranu osobních údajů. *Stanovisko č. 1/2010 ÚOOÚ: Služby soukromých detektivů z pohledu ochrany osobních údajů*. [online]. Aktualizováno srpen 2010. [cit. 31. 3. 2022] Dostupné z: https://www.uoou.cz/files/stanovisko_2010_1.pdf. s. 3.

zaměstnanec právo na přístup ke všem jeho osobním údajům. Zaměstnanec může po zaměstnavateli požadovat, aby byly jeho nesprávné či neúplné osobní údaje vymazány nebo opraveny.[108]

Právní předpisy blíže neuvádějí, jakou formou má zaměstnavatel informační povinnost splnit. Dle Morávka může zaměstnavatel plnit informační povinnost jakoukoliv formu, kterou uzná za vhodnou. Nabízí se možnosti jako informování zaměstnanců vnitřním předpisem, informování osobně personálním oddělením, vyvěšením písemného sdělení na nástěnce na pracovišti, nebo zasláním informace do e-mailových stránek zaměstnanců. Podstatné je, aby došlo k přímému informování konkrétního zaměstnance.[109] Procházková upozorňuje na to, že právní úprava ani nestanovuje, kdy má být zaměstnavatelem informační povinnost splněna. Zohledníme-li účel právní úpravy a seznámíme se s judikaturou (ESLP i soudů v České republice) či stanovisky ÚOOÚ, dospějeme v obecné rovině k závěru, že informační povinnost by měla být splněna před zavedením monitoringu.[110]

Na základě výše uvedených skutečností spatřuji jako nejvhodnější způsob předání informací zaměstnancům v kombinaci informačních kanálů. U kamerového systému například doporučuji, aby zaměstnavatel splnil informační povinnost prostřednictvím interního předpisu. Dále spatřuji jako vhodné zaškolit zaměstnance přijímajícím personalistou. V neposlední řadě doporučuji vyvěšení informační cedule s textem *„prostor je kamerově monitorován“*.

3. 4 Přeshraniční předávání osobních údajů zaměstnanců

Ve spojení s technologickým rozvojem, globalizací a zvýšenou mobilizací občanů se čím dál tím častěji setkáváme na českém pracovním trhu s nadnárodními společnostmi. Ty zde rozvíjejí své ekonomické aktivity prostřednictvím dceřiných společností. Lze logicky očekávat, že dceřiné společnosti budou muset sdílet osobní údaje zaměstnanců se svou mateřskou společností. Předávání osobních údajů je pro rozvoj mezinárodního obchodu a mezinárodní spolupráce nezbytné (bod 101

[108] Rozsudek Evropského soudu pro lidská práva ze dne 12. ledna 2016, stížnost č. 61496/08, BĂRBULESCU proti Rumunsku, s. 26.
[109] MORÁVEK, J. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy,* 17/2017, s. 573. [online]. Publikováno 2017. [cit. 31. 3. 2022]. Dostupné z: https://www.spolpracsoc.cz/files/2018/04/Mor%C3%A1vek-Kontrola-a sledov%C3%A1n%C3%AD-zam%C4%9Bstnanc%C5%AF-%E2%80%93-v%C3%BDklad-%C2%A7-316-ZPr-.pdf.
110 PROCHÁZKOVÁ, E. Několik poznámek k monitoringu zaměstnanců. *Epravo.cz.* [online]. Publikováno 11. 10. 2017 [cit. 2022-03-23]. Dostupné z: https://www.epravo.cz/top/clanky/nekolik-poznamek-k-monitoringu-zamestnancu-106512.html.

recitálu GDPR). Takovéto předání osobních údajů nebude komplikované, bude-li se jednat o předávání údajů mezi státy Evropského hospodářského prostoru[111]. Zde se totiž uplatní zásada volného pohybu údajů. Odlišná situace však nastane, bude-li zaměstnavatel z České republiky předkládat údaje svých zaměstnanců např. managementu do Japonska, tedy země mimo území Evropského hospodářského prostoru. I v takovém případě je GDPR vyžadováno, aby byla ochrana osobním údajům zachována a přeshraničním převodem nebyla ochrana osobních údajů nikterak oslabena (bod 101 recitálu GDPR). I to je důvodem, proč problematiku předávání osobních údajů do třetích zemí upravuje čl. 44 až čl. 50 GDPR.

Pro předávání osobních údajů zaměstnance musí mít zaměstnavatel platný právní důvod. Typickým příkladem je situace, kdy zaměstnavatel (dle GDPR správce) bude zasílat průvodní dotazník přijatého uchazeče. Na základě průvodního dotazníku je zahraničí mateřskou společností (správcem) vystavena pracovní smlouva. Kromě toho mohou být také zaměstnanci zřízeny kupř. přístupové údaje k informačním systémům zaměstnavatele. Jak již bylo uvedeno výše, vždy bude pro zaměstnavatele rozhodující, do jakého státu jsou osobní údaje zaměstnance předávány. V situaci, kdy Evropská komise (dále také „Komise“)[112] rozhodne, že konkrétní stát zajišťuje úroveň ochrany odpovídající požadavkům GDPR (čl. 45 odst. 1 GDPR), může dojít k předání osobních údajů do tohoto státu *de facto* za shodných podmínek, jako mezi státy Evropského hospodářského prostoru. Jarolímková v komentáři k ustanovení uvádí, že pokud Komise vydá rozhodnutí o odpovídající úrovni ochrany, nebude u předávání osobních údajů zapotřebí žádného dalšího povolení od Komise či ÚOOÚ.[113] Před vydáním rozhodnutí Komise vyhodnocuje např. to, jaké má stát přijímající citlivé osobní údaje právní předpisy, zda dodržuje lidská práva a základní svobody či zda v daném státu působí účinný nezávislý dozorový orgán apod. (čl. 45 odst. 2 GDPR). Mezi státy, o kterých

[111] Seznam zemí zařazených do EHP je k dispozici například zde: https://www.kb.cz/getmedia/6ac33196-62a7-423b-8841-667680dfa6ff/Seznam-Zemi-EU-EHP-SEPA.pdf.aspx.
[112] Evropská komise je výkonným orgánem EU.
[113] JAROLÍMKOVÁ, A. In: UŘIČAŘ, M., RÁMIŠ, V. a kol. *Obecné nařízení o ochraně osobních údajů*. 1. vydání. Praha: C. H. Beck, 2021, s. 952–953, marg. č. 8. Článek 45 [Předání založené na rozhodnutí o odpovídající ochraně].

Komise takovým způsobem již v minulosti rozhodla, se řadí např. Japonsko[114], Izrael[115] či Nový Zéland[116].

Nerozhodne-li Komise o tom, že stát zajišťuje úroveň ochrany odpovídající požadavkům GDPR, musí být k dispozici vymahatelná práva a účinná ochrana subjektu údajů (čl. 46 odst. 1 GDPR). V odstavci druhém článku 46 GDPR je uvedeno, pomocí čeho jsou vhodné záruky stanoveny. Tyto záruky jsou rozděleny na ty, které mohou být stanoveny bez zvláštního povolení (čl. 46 odst. 2 GDPR) dozorového úřadu (v České republice ÚOOÚ) a na ty, pro které je zvláštní povolení potřebné (čl. 46 odst. 3 GDPR). Vzhledem k tomu, že GDPR vyjmenovává velké množství těchto záruk, domnívám se, že není možné, a to i s ohledem na rozsah této práce, věnovat prostor všem zárukám. Rozhodla jsem se proto, že pozornost budu dále věnovat pouze podnikovým pravidlům. Ta jsou dle ÚOOÚ vhodným nástrojem pro přeshraniční předávání osobních údajů především u velkých nadnárodních korporací. Vzhledem k tomu, že na našem území zaměstnává zaměstnance velké množství nadnárodních korporací, domnívám se, že bude praktické zaměřit pozornost právě na podniková pravidla. Přeshraničnímu předávání osobních údajů zaměstnanců a dalším vhodným zárukám se chystám věnovat ve svém dalším bádání.

3. 4. 1 Podniková pravidla

Ve vztahu k zaměstnavatelům budou dle mého názoru velmi často užívána závazná podniková pravidla (anglicky *Binding Corporate Rules*, dalé také jako *„BCR"*). Podrobné obsahové náležitosti těchto podnikových pravidel stanovuje čl. 47 GDPR. Burian s Radičovou dále doporučují, aby byla správci údajů (zaměstnavateli) čerpána inspirace z jednotlivých doporučení pracovní skupiny WP29. V těchto doporučeních lze hledat podrobné informace o základních principech podnikových pravidel i to, jak by taková pravidla měla být tvořena. Mohou tak posloužit jako aplikační pomůcka pro nadnárodní korporace při vytváření pravidel.[117]

[114] Prováděcí rozhodnutí Komise ze dne 23. ledna 2019 podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající ochraně osobních údajů poskytované Japonskem na základě zákona o ochraně osobních informací.
[115] Rozhodnutí Komise ze dne 31. ledna 2011 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů státem Izrael v souvislosti s automatizovaným zpracováním osobních údajů.
[116] Prováděcí rozhodnutí Komise ze dne 19. prosince 2012 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů na Novém Zélandu.
[117] BURIAN, D., RADIČOVÁ Z. Mezinárodní předávání osobních údajů z pohledu nové regulace ochrany osobních údajů. *Právní prostor.* [online]. Publikováno 13. 4. 2016 [cit. 31. 3. 2022].

Pro lepší orientaci zaměstnavatelů bylo Evropským sborem pro ochranu osobních údajů vydáno Doporučení č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad s úrovní ochrany osobních údajů v EU (dále také jako *„doporučení“*).[118] Toto doporučení stanovuje šest kroků, které by měl vývozce[119] dat podstoupit před tím, než dojde k přeshraničnímu předání osobních údajů. Uplatňovat by je měl tedy při přeshraničním předávání osobních údajů i zaměstnavatel. Kroky jsou následující:

1. **krok** – seznámit se s tím, jaké údaje jsou zaměstnavatelem předávány. Dále je nutné zohlednit požadavek *minimalizace údajů*. Tedy postupovat tak, aby byly předávány pouze údaje relevantní, přiměřené a v nezbytném rozsahu ve vztahu k účelu, pro který jsou předávány a zpracovávány. Domnívám se například, že bude-li dceřiná společnost předávat údaje pro účely zřízení přístupu do systémů mateřské či sesterské společnosti v zahraničí, neměl by zaměstnavatel z ČR předávat údaje o zdravotním stavu svého zaměstnance apod.
2. **krok** – ověřit si, zda nástroje, které zaměstnavatel pro přeshraniční předávání využívá, jsou uvedeny v taxativním výčtu kapitoly V. *Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím* GDPR.
3. **krok** – posoudit, zda v přijímací třetí zemi existují právní předpisy či praxe, která by mohla ponížit účinnost vhodných záruk nástrojů pro přeshraniční předávání konkrétních osobních údajů. Takovou situaci si můžeme názorně představit v kontextu aktuálního dění. Bude-li mateřská společnost, které mají být údaje předány sídlit na Ukrajině, přeshraniční předávání osobních údajů kupř. splní vhodnou záruku v podobě podnikových pravidel. Lze však předpokládat, že za v současné době probíhající války mezi Ruskem a Ukrajinou, budou muset být přijata další opatření, aby byla zajištěna shodná úroveň ochrany předávaných osobních údajů. V době válečného konfliktu, kdy Ukrajina směřuje veškerou svou pozornost k obraně

Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/mezinarodni-predavani-osobnich-udaju-z-pohledu-nove-regulace-ochrany-osobnich-udaju.

[118] Europion Data Protection Board. *Doporučení č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soudlad s úrovní ochrany osobních údajů v EU*. [online]. Přijato 10. 11. 2020 [cit. 31. 3. 2022]. Dostupné z: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_cs.pdf.

[119] Vývozcem je dle tohoto doporučení myšlen správce či zpracovatel, soukromé subjekty či veřejné orgány, které zpracovávají osobní údaje spadající do oblasti působnosti GPDR.

vlastního území lze totiž oprávněně předpokládat, že úroveň ochrany předávaných osobních údajů bude tímto vojenským konfliktem oslabena.

4. **krok** – určit a přijmout další opatření, která jsou nezbytná pro zajištění úrovně ochrany předávaných údajů. Opatření mají sjednocovat úroveň se standardy kladenými právem EU, a to především s GDPR. Tato opatření mohou být technické, smluvní či organizační povahy (bod 47 doporučení). Nástin těchto opatření tvoří přílohu 2 doporučení. Domnívám se, že je možná jednotlivá opatření též kombinovat, a to v takové míře, aby byla zajištěna dostatečná úroveň ochrany.
5. **krok** – podniknout veškeré kroky v rámci formálního postupu.
6. **krok** – opětovně vyhodnocovat úroveň ochrany zajištěné předávaným osobním údajům. Zaměstnavatel tak má v pravidelných intervalech vyhodnocovat, zda je přeshraniční předávání osobních údajů do třetích zemí v souladu s GDPR.

Podniková pravidla využívá např. společnost GSK. Tato společnost má závazná podniková pravidla pro mezinárodní předávání osobních údajů do zemí mimo Evropský hospodářský prostor a dále pro mezinárodní předávání osobních údajů do Spojeného království.[120] Podniková pravidla využívá též společnost Shell. Shell umožňuje mezinárodní převod osobních údajů zaměstnanců. U této společnosti dochází k přeshraničnímu převodu osobních údajů zaměstnanců za účelem činnosti oddělení lidských zdrojů. Jedná se například o situaci, kdy za účelem zpracovávání žádostí o zaměstnání jsou předávány osobní údaje zaměstnance za účelem nezbytného plnění či správy smlouvy zaměstnance (čl. 8. 2 podnikových pravidel společnosti Shell).[121] Jarolímková v komentáři k ustanovení upozorňuje, že problematická může být otázka vymahatelnosti a závaznosti podnikových pravidel. Jarolímková zaměstnavatelům proto doporučuje, aby byla závaznost aplikována zaměstnavateli v praxi. Tím míní především to, aby byli konkrétní členové korporátních skupin, ale i zaměstnanci nuceni podniková pravidla dodržovat. Toho lze docílit nejen konkrétním efektivním informováním zaměstnanců, ale také třeba zavedením disciplinárních sankcí či školících

[120] GSK. *GSK Public Statements*. [online]. Publikováno prosinec 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.gsk.com/media/6870/czech.pdf.
[121] Shell.cz. *Shell privacy rulles.* [online]. Publikováno 20. 5. 2019 [cit. 31. 3. 2022]. Dostupné z: https://www.shell.cz/privacy/_jcr_content/par/textimage_68bd.stream/1582033078118/cbd1d82ecc649f343df1032f40f8c661baf6d647/shell-binding-corporate-rules.pdf.

programů.[122] Pravidelné proškolování osob majících přístup k osobním údajům je velmi důležité. Osobní údaje zaměstnanců jsou citlivými daty. Přístup nekvalifikovaných osob k těmto údajům je nežádoucí. Jarolímková doporučuje odborná školení upravovat dle konkrétních pozic. Podrobnější školení budou potřebovat zaměstnanci HR oddělení, kteří pracují s osobními údaji pravidelně. Odlišně školeni budou např. techničtí pracovníci.[123]

[122] JAROLÍMKOVÁ, A. In: UŘIČAŘ, M., RÁMIŠ, V. a kol. *Obecné nařízení o ochraně osobních údajů.* 1. vydání. Praha: C. H. Beck, 2021, s. 976, marg. č. 14. Článek 47 [Závazná podniková pravidla].

[123] JAROLÍMKOVÁ, A. In: UŘIČAŘ, M., RÁMIŠ, V. a kol. *Obecné nařízení o ochraně osobních údajů.* 1. vydání. Praha: C. H. Beck, 2021, s. 976, marg. č. 14. Článek 47 [Závazná podniková pravidla].

4 Komparace

Každý ze členských států Evropské Unie je vázán právními normami unijního práva. Právní úprava monitoringu je však napříč členskými státy nejednotná. V této kapitole se zaměřuji na právní úpravu Německa a Finska. Finská právní úprava se věnuje monitoringu zaměstnanců oproti jiným členským státům podrobněji. Ve vztahu k zaměstnavatelům klade přísnější požadavky, než které vyplývají z GDPR. Analýzu německé právní úpravy jsem zvolila z důvodu praktičnosti. Německo je naším sousedním státem, do kterého naši občané často dojíždějí za prací. Na rozdíl od České republiky má Německo obsáhlou judikaturu zabývající se monitoringem zaměstnanců. Právní úprava Německa přitom není oproti naší právní úpravě natolik odlišná. Domnívám se tedy, že by mohla německá právní úprava posloužit jako inspirace pro budoucí vývoj právní úpravy monitoringu v tuzemsku.

4. 1 Finsko

Rozhodla jsem se finskou právní úpravou zabývat především proto, neboť lze tento stát označit za jeden z mála členských států EU, který využil oprávnění vyplývajícího členským státům ze článku 88 GDPR. Oproti České republice stanovil konkrétnější pravidla monitoringu zaměstnanců. Eklundová kupř. uvádí, že finská právní úprava, resp. finské právní předpisy vztahující se k monitoringu, stanovují pro zaměstnavatele významně přísnější kritéria, než ta, která zaměstnavatelům vyplývají z rozhodovací praxe Evropského soudu pro lidská práva či ze stanovisek a dokumentů Pracovní skupiny zřízené podle článku 29.[124] Právní úpravu monitoringu ve Finsku tvoří především GDPR, zákon o ochraně osobních údajů (*Data Protection Act (1050/2018), org. Tietosuojalaki/Dataskyddslag (1050/2018)*)[125] a zákon o ochraně soukromí v pracovním životě (*Act on the Protection of Privacy in Working*, org. *Laki yksityisyyden suojasta työelämässä* (13.8.2004/759), (dále také jako „ZOSVPŽ“).[126]

[124] Eklund, M. C. Monitoring employees' e-mail correspondence and Internet use – A Finnish perspective – PART I. *European Labour Law Journal*, 2019, 10(2), s. 116–133. DOI: 10.1177/2031952519852110.

[130] FinLex. *1050/2018.* [online]. Publikováno 5. 12. 2018. [cit. 31. 3. 2022]. Dostupné z: https://www.finlex.fi/fi/laki/alkup/2018/20181050.

[126] FinLex. *13.8.2004/759.* [online]. Publikováno 13. 8. 2004. [cit. 31. 3. 2022]. Dostupné z: https://www.finlex.fi/fi/laki/ajantasa/2004/20040759. Anglický překlad dostupný z: https://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf.

Právě poslední ze shora uvedených právních pramenů považuji za nejdůležitější, proto se na něj v této kapitole blíže zaměříme. Zákon o ochraně soukromí v pracovním životě představuje *lex specialis* vůči zákonu o ochraně osobních údajů. Stejně jako tuzemská právní úprava (zákon o ochraně osobních údajů a zákoník práce), musí být i finské právní předpisy v souladu v GDPR. Zmíněná právní úprava se vztahuje na všechny zaměstnance, a to jak na zaměstnance v soukromém sektoru, tak na zaměstnance v sektoru státním. Zde můžeme spatřit první významný rozdíl oproti tuzemské právní úpravě. V českém právním řádu nenacházíme žádnou právní normu, která by samostatně upravovala ochranu soukromí zaměstnanců.

Z hlediska zpracovávané problematiky je klíčová především 5. kapitola Kamerový dohled na pracovišti (org. *Kameravalvonta työpaikalla*) zákona o ochraně soukromí v pracovním životě. Tato kapitola upravuje monitoring zaměstnanců prostřednictvím kamerového systému. Dále 6. kapitola Vyzvedávání a otevírání e-mailů patřících zaměstnavateli (org. *Työnantajalle kuuluvien sähköpostiviestien hakeminen ja avaaminen*) zákona o ochraně soukromí v pracovním životě. Tato kapitola upravuje monitoring e-mailových zpráv zaměstnanců. Nyní již samostatně ke konkrétním formám monitoringu.

4. 1. 1 Monitoring zaměstnanců prostřednictvím kamerového systému

Zaměstnavatelé ve Finsku mohou provozovat systém nepřetržitého dohledu kamerovým systémem za účelem zajištění bezpečnosti zaměstnanců či dalších osob v prostorách zaměstnavatele (např. zákazníci, obchodní partneři, klienti apod.). Dalším účelem může být ochrana majetku, přičemž bude kamerovým systémem dohlíženo nad řádným výkonem výrobních procesů. V neposlední řadě také za účelem vyšetřování situací ohrožujících bezpečnost, majetek zaměstnavatele či jeho výrobních procesů. (kapitola 5 ust. §16 odst. 1 ZOSVPŽ). Naopak zaměstnavatel by neměl využívat kamerový systém na pracovišti za účelem dohledu nad konkrétními zaměstnanci. Dále nesmí být kamerový systém využíván ke snímání toalet, šaten či jiných podobných míst či zařízení, které jsou určeny pro osobní potřebu zaměstnanců (kapitola 5 ust. § 16 odst. 1 ZOSVPŽ). Zde můžeme shledat shodu s českou judikaturou, konkrétně v rozsudku Nejvyššího správního soudu České republiky ze dne 23. srpna 2013, sp. zn. 5 As 158/2012. Nejvyšší správní soud zde na 24. straně rozsudku uvedl, že využívá-li zaměstnavatel

k monitoringu zaměstnanců kamerový systém, měly by být tyto kamery namířeny na majetek zaměstnavatele, nikoliv na osobu zaměstnance. Dále říká, že nelze monitoring provádět na místech, které slouží k hygieně či odpočinku zaměstnanců.

Finská právní úprava poskytuje výklad pojmu *závažný důvod*, neboť ho ve svém ustanovení přímo definuje. Česká právní úprava nikoliv. Tuzemská úprava pouze uvádí, že závažný důvod spočívá ve zvláštní činnosti zaměstnavatele (§ 316 odst. 2 ZP) a ponechává interpretaci tohoto neurčitého pojmu na soudech. Osobně dospívám k závěru, že není vhodné pojem *závažný důvod* taxativně vymezovat. Domnívám se, že s ohledem na technologický vývoj, může být právní norma brzy zastaralá a bude ji nutné brzy novelizovat. Toto by mohlo vést ke zbytečnému zahlcování zákonodárců a neefektivitě právní normy, pokud zvážíme také délku legislativního procesu. Naproti tomu spatřuji pozitivum v konkrétní formulaci v rámci finského ustanovení. Důvodem je dle mého názoru snazší interpretace pojmu pro laickou veřejnost.

Zákon o ochraně soukromí v pracovním životě však stanovuje též konkrétní případy, při kterých nemusí být naplněny shora uvedené podmínky pro to, aby mohl zaměstnavatel monitorovat zaměstnance prostřednictvím kamerového systému. Jedná se o následující tři případy:

- V situaci, kdy zaměstnavatel má tímto monitoringem za cíl předejít zjevné hrozbě násilí, která souvisí s činností zaměstnance, nebo předchází-li tím zjevné újmě či ohrožení bezpečnosti či zdraví zaměstnance (kapitola 5 ust. §16 odst. 2. bod 1) ZOSVPŽ). Dle mého názoru by bylo možné pod tento případ podřadit kupř. zaměstnance pracující pro jaderné elektrárny či vojenské výrobní společnosti. Naopak hrozby násilí v rámci pracovní doby čelí příslušníci bezpečnostních sborů při provádění bezprostředních zásahů, osobní bodyguardi či ostraha u nočních klubů a heren. Jedna z takových situací se stala v roce 2022 v České republice, kde byl napaden člen ostrahy obchodu zákazníkem, za to, že v souladu s nařízením vlády zamezil zákazníkovi vstupu do prodejny z důvodu nenasazeného respirátoru.[127]
- Pro potřeby prevence či vyšetřování majetkové trestné činnosti. To však pouze za situace, pokud je nezbytnou součástí pracovní činnosti zaměstnance manipulace s majetkem vysoké hodnoty (kapitola 5 ust. §16

[127] Novinky.cz. *Muž zmlátil ochrankáře, který ho nechtěl pustit do obchodu bez respirátoru.* [online]. Publikováno 11. 1. 2022. [cit. 31. 3. 2022]. Dostupné z: https://www.novinky.cz/krimi/clanek/muz-zmlatil-ochrankare-ktery-ho-nechtel-pustit-do-obchodu-bez-respiratoru-40383575.

odst. 2. bod 2) ZOSVPŽ). Majetkem vysoké hodnoty se rozumí např. peníze, cenné papíry či jiné cennosti.

- Posledním případem je pak situace, kdy je kamerový systém instalován na ochranu zájmů a práv zaměstnance a na žádost zaměstnance, který je předmětem takového sledování (kapitola 5 ust. §16 odst. 2. bod 3) ZOSVPŽ). Ve Finsku je tedy možné, aby byl kamerový systém zaveden a například i na konkrétního zaměstnance namířen tehdy, bude-li si to zaměstnanec výslovně přát. Domnívám se, že taková situace by mohla nastat například u lékaře provádějícího operaci za účelem zamezení případně později vzniknuvších sporů mezi pacientem a lékařem či jeho rodinnými příslušníky. Stejně tak by mohl požádat o zavedení kamerového sledování například strojvůdce osobního vlaku, který nese odpovědnost za cestující. Záznam z kamerového systému by mohl v případě dopravní nehody posloužit jako podpora jeho tvrzení. Dokážu si však představit i další pozitiva. Řadím mezi ně, například lepší komunikaci s dispečinkem vlakové dopravy v případě technických problémů či při zdravotní indispozici strojvůdce.

Velice zajímavé je ustanovení § 17 Zákona o ochraně soukromí v pracovním životě. Toto ustanovení umožňuje zaměstnavateli používat video nahrávky jako důkazní materiál dokládající naplnění důvodu pro ukončení pracovního poměru. Dospívám však k závěru, že tato možnost může mít též negativní důsledky. V absurdní situaci by mohl zaměstnavatel prostřednictvím kamerového záznamu vyčkávat na první selhání zaměstnance. Z české právní úpravy (zákoník práce, zákon o ochraně osobních údajů) zmocnění k užití záznamu z kamerového systému zaměstnavateli nevyplývá. Dále lze konstatovat, že není v žádné z právních norem přímo řečeno, že by mohl záznam z kamerového systému sloužit jako důkaz.

Pouze ustanovení § 125 českého zákona č. 99/1963 Sb., občanský soudní řád, v platném znění stanovuje, že jako důkazní prostředek může sloužit jakýkoliv prostředek, jímž lze zjistit stav věci. Problematikou užití kamerového záznamu jako důkazu se zabýval např. Ústavní soud v usnesení ze dne 8. ledna 2019, sp. zn. I. ÚS 3900/18. Předmětem řízení před ÚS bylo určení neplatnosti výpovědi z pracovního poměru. Zaměstnankyně (žalobce) pracovala pro obchodní řetězec. Výpověď byla zaměstnankyni udělena podle § 52 písm. g) ZP. Důvodem pro udělení výpovědi bylo opakované porušování interních předpisů, nedodržování pracovní doby či prodlevy nesouvisející s výkonem práce. Zaměstnankyně jako vedoucí pobočky

trávila většinu své pracovní doby povídáním se známými. Zaměstnavatel (žalovaný) u soudu prvního stupně inicioval provedení důkazu přehráním kamerového záznamu z prodejny. Důkazní břemeno v tomto řízení bylo na zaměstnavateli. Kamerový záznam v daném případě nejlépe prokázal skutková tvrzení. Tímto kamerovým záznamem se zaměstnavateli podařilo prokázat skutečnosti, pro které byla výpověď z pracovního poměru uložena. Soud prvního stupně proto žalobu zamítl. Ke stejným závěrům dospěl též soud druhého stupně. Ústavní soud v daném případě ústavní žalobu odmítl. Provedení důkazu záznamem z kamerového systému bylo v souladu se zákonem.

4. 1. 2 Monitoring e-mailových zpráv zaměstnanců

Otevírání zpráv elektronické upravuje kapitola 6 zákona o ochraně soukromí v pracovním životě. Zaměstnavatel má ve Finsku povinnost naplánovat a zajistit nezbytná opatření vedoucí k tomu, aby zaměstnavatel nemusel otevírat či číst zprávy elektronické pošty svých zaměstnanců. Některá z těchto ochranných opatření by mohla sloužit i jako inspirace pro zaměstnavatele v České republice.

V kapitole 18 Povinnosti zaměstnavatele (org. *Työnantajan huolehtimisvelvollisuudet)* finského zákona o ochraně soukromí v pracovním životě (org. *Laki yksityisyyden suojasta työelämässä*) jsou stanovena následující opatření:

- Zaměstnanec má mít možnost využít funkce automatické odpovědi. Odeslat konkrétnímu odesílateli e-mailové zprávy informaci o délce nepřítomnosti adresáta zprávy, dále i informace o osobě, která se má v době nepřítomnosti starat o konkrétní úkoly (kapitola 6 ust. § 18 odst. 1 ZOSVPŽ).
- Zaměstnanec může využít přesměrování e-mailových zpráv na jiného ze svých kolegů, který byl zaměstnavatelem předem schválen či určen, nebo na jinou zaměstnavatelem schválenou adresu zaměstnance (kapitola 6 § 18 odst. 2 ZOSVPŽ). Domnívám se, že jako modelový příklad by mohla posloužit následující situace: Zaměstnavatel zaměstnává tři projektové manažery. Každý z těchto projektových manažerů komunikuje s předem vymezenými dodavateli. V okamžiku nepřítomnosti jednoho ze zaměstnanců, mohou být e-maily od konkrétních adresátů zasílány jinému kolegovi. Kdy tuto volbu může předem stanovit či schválit zaměstnavatel.
- Zaměstnanec sám po předchozím schválení zaměstnavatele určí kolegu, který bude oprávněn v době jeho nepřítomnosti kontrolovat zprávy došlé na jeho pracovní e-mailovou adresu. Tento kolega obdrží od zaměstnance

souhlas k přístupu do jeho e-mailové schránky. V době nepřítomnosti zaměstnance bude tento kolega třídit příchozí e-mailové zprávy. Pokud bude na e-mailovou schránku nepřítomného zaměstnance doručena e-mailová zpráva, která je jednoznačně určena pro zaměstnavatele a jeho pracovní činnost, bude tento kolega oprávněn s ní dále nakládat. Oprávněn je ke zpracovávání těch e-mailových zpráv, u nichž je nezbytné, aby o nich byl zaměstnavatel informován. Bude se tedy jednat například o e-mailové zprávy s fakturami, přístupovými údaji či objednávkami. (kapitola 6 ust. § 18 odst. 3 ZOSVPŽ).

Stejně jako u monitoringu prostřednictvím kamerového systému se také u monitoringu e-mailové korespondence setkáváme s tím, že zaměstnanec sám může *de facto* požadovat, aby byl monitoring prováděn. Dle mého názoru by bylo do budoucna vhodné zapracovat obdobná ustanovení i do naší právní úpravy. Domnívám se, že vytvoření takové právní úpravy přinese jistá pozitiva, jakými jsou kupř. minimalizace šikany na pracovišti či drobných naschválů, které si kolegové v rámci pracovní rivality činí.

V případě, že nebyla aplikována shora uvedená opatření a současně, pokud se jedná se o věc, která nesnese odkladu a nelze-li dosáhnout souhlasu zaměstnance, může zaměstnavatel e-mail otevřít. Zaměstnavatel může takto postupovat pouze za přítomnosti IT specialisty, resp. správce sítě. Za velký přínos bych ráda označila též webové stránky Úřadu ombudsmana pro ochranu osobních údajů.[128] Na těchto stránkách nalezneme vcelku podrobný rozbor jednotlivých forem monitoringu. Domnívám se, že jejich webové stránky by mohly být inspirací pro ÚOOÚ. Aktuální vzhled webových stránek je oproti stránkám Úřadu ombudsmana pro ochranu osobních údajů ve Finsku nepřehledný.

4. 2 Německo

Jako další stát pro komparaci jsem si zvolila sousední Německo. Hlavním důvodem je, že mnozí občané ČR za prací do Německa dojíždějí. Např. v roce 2019 překročil počet pracujících Čechů v Německu 37 tisíc.[129] Považuji proto za přínosné, aby byla část této kapitoly věnována též německé právní úpravě. Mezi

[128] Tietosuojavaltuutetun Toimisto. *Oikopolkuja.* [online]. Publikováno © 2022. [cit. 31. 3. 2022]. Dostupné z: https://tietosuoja.fi.

[129] ČT 24. *Za prací dojíždí do ciziny přes 56 tisíc Čechů. Nejvíc do Německa, míří ale i do Británie.* [online]. Publikováno 2. 9. 2019. [cit. 31. 3. 2022]. Dostupné z: https://ct24.ceskatelevize.cz/ekonomika/2912609-za-praci-dojizdi-do-ciziny-pres-56-tisic-cechu-nejvic-do-nemecka-miri-ale-i-do.

nejvýznamnější právní předpisy upravující problematiku monitoringu zaměstnanců v Německu řadíme především federální zákon o ochraně údajů, (org. *Bundesdatenschutzgesetz,* dále také jako „BDSG"). Ve vztahu k monitoringu však nelze opomenout článek 10 odst. 1 Základního zákona spolkové republiky Německo (org. *Grundgesetz für die Bundesrepublik Deutschland*),[130] jež poskytuje ochranu korespondenci a telekomunikacím. Dále je třeba v souvislosti s probíranou problematikou uvést zákon o telekomunikacích (org. *Telekommunikationgesetz,* dále také jako „TKG") [131]. Tento dokument poskytuje ochranu telekomunikačnímu tajemství. V neposlední řadě mezi základní právní úpravu vážící se tomuto tématu patří také zákon o telemédiích (org. *Telemediegesetz,* dále také jako „TMG")[132].

Německé úřady pro ochranu údajů totiž považují zaměstnavatele, kteří umožňují zaměstnanci užívání telekomunikačních systémů pro osobní účely, za poskytovatele telekomunikačních služeb dle TKG nebo poskytovatele telemediálních služeb dle TMG. Tato úprava je pro německé zaměstnavatele problematická. TKG obecně zakazuje poskytovatelům telekomunikačních služeb monitorovat komunikaci jednotlivců. Naproti tomu TMG obvykle zabraňuje poskytovatelům telemediálních služeb zpracovávat informace o přístupu jednotlivců na webové stránky.

Vrátíme-li se zpět k právní úpravě obsažené v BDSG, lze za klíčové označit § 26 tohoto zákona. Například druhá část prvního odstavce stanovuje, že osobní údaje zaměstnanců mohou být zpracovávány za účelem odhalování trestných činů pouze v případě, že existuje důvodná obava, že zaměstnanec v rámci zaměstnání spáchal trestný čin. Dále mohou být osobní údaje tímto způsobem zpracovány, je-li zpracování těchto údajů nezbytné pro vyšetřování trestného činu a nepřevažuje-li oprávněný zájem zaměstnance na tom, aby tyto údaje zpracovávány nebyly (§26 BDSG). Samozřejmě druh a rozsah takového zpracování nesmí být nepřiměřený důvodu. V souvislosti s tím si dovolím opětovně odkázat na již zmiňované rozhodnutí Federálního pracovního soudu (org. *Bundesarbeitsgericht*, dále také

[130] Bundesministerium der Justiz. Bundesamt für Justiz. *Grundgesetz für die Bundesrepubklik Deutschland.* [online]. Změněno 29. 9. 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.gesetze-im-internet.de/gg/BJNR000010949.html.

[131] Bundesministerium der Justiz. Bundesamt für Justiz. *Telekommunikationgesetz.* [online]. Publikováno 23. 6. 2021. [cit. 31. 3. 2022]. Dostupné z: https://www.gesetze-im-internet.de/tkg_2021/.

[132] Bundesministerium der Justiz. Bundesamt für Justiz. *Telemediegesetz.* [online]. Publikováno 26. 2. 2007. [cit. 31. 3. 2022]. Dostupné z: https://www.gesetze-im-internet.de/tmg/.

jako „BAG“) ze dne 27. července 2017, sp. zn. 2 AZR 681/16. V tomto rozhodnutí BAG dospěl k názoru, že záznam z keyloggeru byl získán v rozporu s BDSG.[133]

Ustanovení § 26 odst. 3 BDSG zaměstnavatelům umožňuje zpracovávat též odchylně od čl. 9 odst. 1 GDPR tzv. zvláštní kategorii osobních údajů. Do skupiny zvláštní kategorie osobních údajů můžeme řadit např. myšlenky, dále osobní údaje vypovídající např. o politických názorech, náboženském vyznání, ale také zpracování genetických či biometrických údajů. Německá právní úprava umožňuje tyto údaje zaměstnavatelům zpracovávat, ovšem pouze za předpokladu, že jsou tyto údaje nezbytné pro výkon práv či dodržování zákonných povinností. Tyto povinnosti vyplývají z norem německého pracovního práva, norem práva sociálního zabezpečení, nebo z důvodů sociální ochrany. Výjimku tvoří situace, kdy převažuje oprávněný zájem zaměstnance, aby tyto údaje zpracovány nebyly. Německo tak odchylně od České republiky využilo výjimky, kterou článek 9 odst. 2 písm. b) GDPR umožňuje. Zde bych si dovolila upozornit na snahy ÚOOÚ. ÚOOÚ v roce 2019 navrhl ministerstvu práce a sociálních věcí České republiky změny v zákoníku práce.[134] ÚOOÚ navrhoval, aby bylo za § 316 ZP vloženo nové ustanovení §316a pojednávající o biometrických údajích zaměstnanců.

Zaměstnavatel měl být dle tohoto návrhu oprávněn využívat biometrické údaje za účelem ochrany výrobních a pracovních prostředků a technologií. Zaměstnavatel měl mít dle tohoto návrhu možnost využít biometrické údaje k identifikaci konkrétního zaměstnance. Tyto biometrické údaje se měly dle ÚOOÚ vztahovat pouze na ty biometrické údaje, které používají morfologické znaky zaměstnanců.[135] Morfologickými znaky jsou dle Prouzy myšleny např. digitální otisk či scan žilního systému ruky.[136] Využity pak dle ÚOOÚ mohly být pouze za účelem kontroly přístupu k výrobním či jiným provozním zařízením zaměstnavatele a dále k přístupu do objektů zaměstnavatele či jednotlivých částí, kde jsou tato zařízení umístěna. Novela zákoníku práce však tyto změny nepřinesla.

---

[133] Poznámka autora: rozsudek odkazuje na § 32 BDSG, současná platná právní úprava obsahuje toto v § 26 odst. 2 BDSG.

[134] Úřad pro ochranu osobních údajů. *ÚOOÚ navrhuje změny v oblasti zpracování biometrických údajů zaměstnanců.* [online]. Publikováno 30. 7. 2019. [cit. 31. 3. 2022]. Dostupné z: https://www.uoou.cz/uoou-navrhuje-zmeny-v-oblasti-zpracovani-biometrickych-udaju-zamestnancu/d-35406.

[135] Úřad pro ochranu osobních údajů. *Připomínka, č.j. UOOU-02950/19-4.* [online]. Publikováno 29. 7. 2019. [cit. 31. 3. 2022]. Dostupné z: Návrh ke změně zákona dostupný zde: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=35418, s. 2.

[136] PROUZA, J. Zpracování biometrických údajů zaměstnanců. *Epravo.cz.* [online]. Publikováno 22. 8. 2019. [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-zamestnancu-109845.html.

Osobně se domnívám, že je to velká škoda, a to i s ohledem na současnou politickou situaci. Ta poukazuje na to, že důležité státní statky, jako jsou elektrárny či zbrojní a vojenský průmysl, by měly být zabezpečeny v maximální možné míře.

Na druhou stranu je však nutno poukázat na rozhodovací praxi ÚOOÚ, který říká, že zpracovávání biometrických údajů by mělo být využíváno pouze výjimečně. V praxi se s nimi setkáváme například u docházkových systémů. U docházkových systémů mohou být biometrické údaje využívány za předpokladu, že nepostačuje prostá evidence osob. Zaměstnavatel tedy bude mít odůvodněný zájem na tom, aby byla identifikace jednoznačná a nemohlo dojít k pochybení v osobě zaměstnance.[137] ÚOOÚ pak na základě tohoto např. vyvodil, že užití docházkového systému s aplikací face-ID[138] ve stavebnictví je možné. Staveniště je totiž pracoviště specifického charakteru. Je v zájmu zaměstnavatele i zaměstnance, aby byla zajištěna bezpečnost a ochrana života a zdraví při práci.[139] Stanovisko ÚOOÚ je příkladem toho, že ačkoliv v současné právní úpravě nenacházíme obdobnou úpravu té německé, lze vidět, že ÚOOÚ přistupuje k užívání biometrických údajů rozumně. Zaměstnavatel, který dostatečně odůvodní užití biometrických údajů, se tak dle mého názoru nemá důvod obávat sankce.

Ustanovení § 26 odst. 2 BDSG se věnuje institutu souhlasu zaměstnance. Zde je nutné opět primárně odkázat na úpravu obsaženou v GDPR, s nímž musí být souhlas v souladu. Respektive v souladu s požadavky kladenými ve článku 4 odst. 11 GDPR. Musí být tedy souhlasem svobodným, informovaným a jednoznačným. Musí se tedy jednat o souhlas, kterým bude jakýmkoliv svobodným, informovaným, jednoznačným projevem vůle, jímž bude zaměstnanec dávat svolení ke zpracování osobních údajů. Dle čl. 6 odst. 1 písm. a) GDPR musí být souhlas udělen k jednomu či více konkrétních účelů. Zaměstnavatelé v Německu musí interpretovat tyto články právě v souvislosti s § 26 odst. 2 BDSG. Dle tohoto ustanovení se při posuzování, zda byl udělen souhlas svobodně, přihlédne především k míře závislosti zaměstnance v rámci pracovněprávního vztahu. Dále se také přihlédne k okolnostem, za kterých byl tento souhlas zaměstnavateli udělen.

Ustanovení § 26 odst. 4 BDSG umožňuje, aby byla bližší pravidla zpracování osobních údajů zaměstnanců stanovena v kolektivních smlouvách.

[137] Protokol o kontrole ÚOOÚ ze dne 9. ledna 2019, č.j. UOOU-09072/18-14, s. 8.
[138] Jedná se o aplikaci umožňující rozpoznání zaměstnance na základě snímání jeho obličeje. Na základě takto pořízeného snímání pak vyhodnotí, zda se jedná o osobu, jíž je přístup na pracoviště povolen či zakázán.
[139] Srov. protokol o kontrole ÚOOÚ ze dne 9. ledna 2019, č.j. UOOU-09072/18-14.

V kolektivních smlouvách by měla být také zpracována zvláštní kategorie osobních údajů zaměstnanců.

Základ pro oprávnění zaměstnavatele sledovat zaměstnance představují též ustanovení § 241 a § 242 německého občanského zákoníku (org. *Bürgerliches Gesetzbuch,* dále také jako „BGB“). Tato ustanovení definují závazkový vztah. Ustanovení § 241 odst. 1 BGB uvádí, že je oprávněný oprávněn požadovat po povinném plnění. Tedy zaměstnavatel je oprávněn po zaměstnancích požadovat, aby plnili kromě svých pracovních úkolů, také úkoly spočívající v ochraně zaměstnavatelových oprávněných zájmů (například související s výkonem jeho vlastnického práva). Odstavec druhý téhož ustanovení dále stanovuje, že závazek může dle svého obsahu zavazovat druhou stranu (v daném případě zaměstnance či zaměstnavatele) k tomu, aby přihlížela k oprávněným zájmům a právům první ze zmíněných stran (§ 241 odst. 2 BGB). Dle ustanovení § 242 BGB pak má být závazek povinným plněn v souladu s požadavky dobré víry, zvyklostí a s přihlédnutím k obvyklé praxi. Ustanovení § 87 odst. 1 bodu 6 zákona o pracovních vztazích v podnicích (org. *Betriebsverfassungsgesetz,* dále také jako „BV“) ukládá podnikové radě právo spolurozhodovat o tom, zda může zaměstnavatel zavést a používat technická zařízení ke sledování chování nebo výkonu zaměstnanců. Podnikové rady jsou v Německu ustavovány v podnicích s nejméně pěti stálými zaměstnanci (§ 1 odst. 1 BV).

Federální zákon o ochraně údajů se na rozdíl od finského zákona o ochraně soukromí v pracovním životě výslovně nevyjadřuje k možnosti zaměstnavatelů monitorovat určité typy činností zaměstnanců. Domnívám se však, že by se i přesto měli němečtí zaměstnavatelé vyhýbat monitoringu míst, kde zaměstnanci přiměřeně očekávají míru soukromí (bude se tak jednat o šatny, toalety aj.).

Německé zákony obecně nevyžadují souhlas zaměstnance s monitoringem, pokud zaměstnavatel nepovolí osobní používání svých komunikačních systémů. V případě, že zaměstnavatel používání komunikačních systémů k osobním účelům povolí, může zaměstnanec uložit zaměstnavateli buď svůj souhlas s podmínkou, dále může souhlas odepřít, anebo má možnost se zdržet osobního užívání komunikačních systémů zaměstnavatele. V případě udělení souhlasu s podmínkou může zaměstnanec zaměstnavateli sdělit, že bude využívat komunikačních systémů zaměstnavatele k osobním účelům.

4. 2. 1 Monitoring e-mailové adresy a internetové aktivity zaměstnance

Monitoring využívání e-mailových adres a internetové aktivity zaměstnance je nutné posuzovat dle toho, zda zaměstnavatel umožnil zaměstnancům využívat e-mail a internetové služby k osobním účelům či nikoliv. Jak uvádí Prestel s Kellerem, v případě, kdy zaměstnanec souhlas s užíváním e-mailových schránek či internetových služeb neudělí, se nebude na zaměstnavatele nahlížet jako na poskytovatele služeb ve smyslu TKG. Postupovat se tak bude v souladu s BDSG.[140] A to především v souladu s § 26 BDSG, kterému byla již v této kapitole věnována bližší pozornost.

V případě, kdy zaměstnavatel udělí zaměstnanci svolení s užíváním e-mailové schránky k osobním účelům, bude se aplikovat též TKG. Zaměstnavateli je odepřen přístup i k pracovním e-mailům, pokud nelze soukromé e-maily odlišit od pracovních.[141] Na soukromé e-maily se v tomto případě budou vztahovat ustanovení TKG. Zaměstnavatel, stejně jako jakýkoliv jiný poskytovatel telekomunikačních služeb, není oprávněn odposlouchávat (či jinak sledovat) komunikaci svého zákazníka, v tomto případě hovoříme o osobě zaměstnance. Existují však dvě výjimky. První výjimkou je udělení výslovného souhlasu zaměstnancem. Druhá výjimka upravuje situaci, kdy je důvodné podezření, že zaměstnanec spáchal trestný čin a účelem tohoto sledování je vyšetřování takového trestného činu. V okamžiku, kdy zaměstnavatel naopak udělí souhlas zaměstnanci s užíváním internetu k soukromým účelům, nesmí takové užívání významně zhoršovat výkon práce, která má být zaměstnancem odvedena.[142]

4. 2. 2 Monitoring prostřednictvím kamerového systému

Právní základ monitoringu kamerovými systémy nacházíme v německé právní úpravě v BDSG, a to ve dvou následujících ustanoveních. První z ustanovení upravuje snímání veřejně přístupných prostranství kamerami (§ 4 BDSG). Dále je v souvislosti s tímto tématem nutno zmínit také § 26 BDSG. Ten stanovuje,

[140] PRESTEL, Patrick a Max-Lion KELLER. Überwachung und Kontrolle des Arbeitnehmers und die Konflikte mit dem Fernmeldegeheimnis und dem Datenschutz (7. Teil der neuen Serie der IT-Recht Kanzlei zu den Themen E-Mailarchivierung und IT-Richtlinie). *It-recht kanzlei München.* [online]. Publikováno 6. 7. 2010. [cit. 31. 3. 2022]. Dostupné z: https://www.it-recht-kanzlei.de/e-mail-archivierung-%C3%BCberwachung-kontrolle-arbeitnehmer-fernmeldegeheimnis-datenschutz.html.

[141] Tamtéž.

[142] Rozsudek Státního pracovního soudu Berlín – Branderburg ze dne 14. ledna 2016, sp. zn. 5 So 657/15, bod 87.

pro jaké účely mohou být zpracovávány osobní údaje zaměstnanců, a to včetně zvláštní kategorie osobních údajů. Upravuje institut souhlasu zaměstnance a též možnost konkretizace pravidel pro zpracovávání osobních údajů prostřednictvím kolektivních smluv. Chce-li tedy zaměstnavatel v Německu zavést kamerový systém, musí nejdříve určit, zda má být kamerový systém nainstalován na veřejně přístupném prostranství (např. obchodní centra, pohostinství aj.), nebo na místě, které veřejně přístupné není. Intenzita zásahu do soukromí osob a jejich osobnostních práv je nižší u monitoringu veřejně přístupných prostranství než na pracovišti. Je to logické. Na rozdíl od sledování veřejně přístupných prostranství (např. parkoviště, veřejná přístupná sportoviště) jsou na pracovišti monitorovány osoby, které jsou zaměstnavateli známy. Dalším rozdílem je také to, že na veřejně přístupném prostranství je osoba monitorovaná pouze krátkodobě (např. v době, kdy se pohybuje po ploše obchodního střediska), zatímco monitoring zaměstnanců trvá několik hodin, případně i dnů.[143]

V situaci, kdy chce zaměstnavatel zavést monitoring kamerovým systémem na pracovišti, bude se postupovat dle § 26 BDSG. Zpracovávání osobních údajů bude zákonné, bude-li nezbytné pro výkon pracovněprávního vztahu nebo pro odhalování trestných činů spáchaných zaměstnanci.[144] V případě, kdy se bude jednat o instalaci na místě veřejně přístupném, bude se aplikovat § 4 BDSG. Monitoring veřejně přístupných prostranství je možný pouze v nezbytně nutném rozsahu (§4 odst. 1 BDSG). Dále je monitoring veřejně přístupných prostranství možný za účelem plnění úkolů veřejnými orgány (§ 4 odst. 1 bod 1. BDSG), tj. například výkon bezprostředních zásahů příslušníků policie a za účelem ochrany domovního práva (§ 4 odst. 1 bod. 2 BDSG), např. za účelem sledování příjezdové cesty k rodinnému domu.

Pro potřeby monitoringu zaměstnanců je pro zaměstnavatele klíčové § 4 odst. 1 bod. 3 BDSG. Toto ustanovení umožňuje instalaci kamerového zařízení za účelem ochrany oprávněných zájmů, tj. například za účelem ochrany vlastnického práva zaměstnavatele (§ 4 odst. 1 bod. 3 BDSG). BDSG dále stanovuje, že je při monitoringu veřejně přístupných prostranství kamerovým systémem (např. sportovišť, míst určených pro shromažďování a zábavu) ochrana života, zdraví

[143] Rozhodnutí Federálního pracovního soudu ze dne 14. prosince 2004, sp. zn. 1 ABR 34/03, bod 38.
[144] MÖLLER, F. *Video surveillance of employees in Germany: get ready for compliance checks!*. Ius Laboris. [online]. Publikováno 11. 3. 2021. [cit. 31. 3. 2022]. Dostupné z: https://iuslaboris.com/insights/video-surveillance-of-employees-in-germany-get-ready-for-compliance-checks/?.

a svobody považována za velmi důležitý zájem. Domnívám se proto, že v takovém případě bude převažovat zájem na ochranu života, zdraví a svobody kamerovým systémem snímaných jednotlivců nad zájmem na zajištění a ochranu soukromí.

Sledování zaměstnanců musí být nezbytné a vhodné, a to s ohledem na zaměstnanci zaručená práva. Zaváděný monitoring má vést k dosažení zamýšleného účelu. K dispozici nejsou zaměstnavateli žádné další prostředky, které by byly stejně účinné jako zaváděný monitoring a méně omezující osobnostní práva zaměstnance.[145]

Z judikatury německých soudů můžeme vysledovat, že není vyloučeno ani tajné sledování. Nejčastěji je toto tajné sledování instalováno v nákupních střediscích či prodejnách. Důvodem bývá podezření z páchání trestné činnosti, nejčastěji krádeží prováděných zaměstnanci. Zaměstnavatel se nesmí omezit na obecný předpoklad, že by mohlo dojít ke spáchání trestného činu. Naproti tomu jeho podezření by nemělo směřovat proti konkrétnímu zaměstnanci.[146] Může tak být namířeno například vůči všem pokladním. Na pokladnách se totiž personál velmi často obměňuje. Namíření monitoringu jen vůči jedné konkrétní osobě by tak bylo neúčelné a kontraproduktivní. Vždy by měl mít zaměstnavatel důvodné a konkrétní podezření, že dochází k páchání trestné činnosti. Domnívám se, že jako legitimní důvod postačí skutečnost, že zaměstnavatel zjistil opakovaně nesrovnalosti v rámci inventur. Dle Federálního pracovního soudu (org. *Bundesarbeitsgericht)* je zásah do práv zaměstnance přípustný též instalací kamerových systémů. Toto je ovšem možné jen za podmínky, že má zaměstnavatel konkrétní podezření, že dochází k páchání trestné činnosti nebo jinému závažnému pochybení v jeho neprospěch. Jak jsem již zmínila výše, jedná se o řešení, které by mělo představovat tzv. *ultima ratio*. Zaměstnavatel tedy před tím musí vyčerpat všechny méně intenzivní prostředky k vyšetření konkrétního podezření. Teprve až v momentě, kdy je tajné sledování prakticky jediným zbývajícím prostředkem, se k němu smí uchýlit.

V neposlední řadě je také důležité, aby byl zachován požadavek přiměřenosti.[147] Jako mírnější prostředek sledování zaměstnanců se nabízí sledování zaměstnanců prostřednictvím kamerových systémů bez záznamu.

[145] Rozhodnutí Federálního pracovního soudu ze dne 14. prosince 2004, sp. zn. 1 ABR 34/03, bod. 27.
[146] Rozsudek Federálního pracovního soudu ze dne 21. června 2012, sp. zn. 2 AZR 153/11, bod. 38.
[147] Rozsudek Federálního pracovního soudu ze dne 21. listopadu 2013, sp. zn. 2 AZR 797/11, bod. 56.

Tedy takovými kamerovými systémy, jimiž je pořizován v konkrétní okamžik obrazový záznam, ale záznam se neukládá. Tento kamerový záznam může být průběžně kontrolován jiným k tomu určeným zaměstnancem. Kamerový systém bez záznamu zajisté také představuje zásah do soukromí zaměstnance. Domnívám se však, že možnost bez pozdějšího přehrání a zpracování záznamu je méně invazivním zásahem, který může představovat schůdné řešení.[148]

[148] Rozhodnutí Federálního pracovního soudu ze dne 29. června 2004, sp. zn. 1 ABR 21/03, bod. 39 cc.

Závěr

Ve své diplomové práci jsem se zaměřila na *monitoring zaměstnanců ve světle judikatury ČR*. Jedná se o téma velice široké, které nelze s ohledem na rozsah práce vyčerpat. V úvodu této diplomové práce jsem si stanovila za cíl poskytnout základní náhled do problematiky monitoringu zaměstnanců, popsat současný stav a poskytnout ucelený přehled o vybraných formách monitoringu.

Je zřejmé, že se Evropská Unie snaží reagovat na trendy v monitoringu zaměstnanců a zpracovávání osobních údajů, a to přijímáním právních norem. Významnou roli v oblasti monitoringu a zpracovávání osobních údajů zaměstnanců zaujímá též Evropský sbor pro ochranu osobních údajů. Ten je schopen mnohem flexibilněji reagovat na politické a společenské záležitosti (např. na pandemii covid-19)[149] přijímáním různých právních instrumentů. Povědomí o těchto instrumentech mezi zaměstnavateli a zaměstnanci je však dle mého osobního názoru velmi malé. To považuji za velice nešťastnou skutečnost, neboť osobně shledávám dokumenty Evropského sboru pro ochranu osobních údajů jako výbornou interpretační a aplikační pomůcku. Pro lepší pochopení problematiky je však důležité pracovat též s judikaturou. V diplomové práci jsem svou pozornost zaměřila na nejvýznamnější judikáty související s problematikou monitoringu zaměstnanců. Ačkoliv českými soudy dosud velké množství judikátů pojednávajících o monitoringu zaměstnanců nenacházíme, judikatura Evropského soudu pro lidská práva je nosným zdrojem. Především judikatuře ESLP se chystám blíže věnovat při svém dalším bádání.

Moderní technologie i trendy v odvětví lidských zdrojů se neustále vyvíjí. Pandemie onemocnění covid-19 i současný válečný konflikt na území Ukrajiny dokládají to, jak zranitelná a závislá je naše ekonomika na okolním světě. Rychlý vývoj sledujeme též v oblasti moderních technologií. Lze proto očekávat, že zaměstnavatelé budou vyhledávat další možnosti, jak své zaměstnance sledovat a optimalizovat náklady. S rozvojem technologií navíc předpokládám, že v budoucnu budou zaměstnanci potřebovat pro svou práci firemní telefony, internet a jiné prostředky mnohem více než je tomu dnes. Ze shora uvedených důvodu se proto domnívám, že je správné, že máme vymezenou právní úpravu obecně.

[149] Kupř. European Data Protection Board. *Prohlášení o zpracování osobních údajů v souvislosti s výskytem onemocnění covid-19.* [online]. Publikováno 11. 3. 2020. [cit. 31. 3. 2022]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_art_23gdpr_20200602_cs_1.pdf.

Obecná právní úprava totiž dokáže, dle mého názoru, lépe reagovat na vývoj a technologický pokrok. Obzvláště u nás, kde je legislativní proces přijímání zákonů dlouhý.

Za problematické považuji, že je právní úprava monitoringu zaměstnanců roztříštěná mezi mnohé právní předpisy. Je nutné vycházet z toho, že adresáti právních norem jsou především laici a roztříštěnost právní úpravy jim správnou interpretaci a orientaci dosti ztěžuje. Zde bych proto doporučila zákonodárci čerpat inspiraci u finské právní úpravy. Finsko se vydalo cestou přijetí komplexnějšího zákona, ve kterém jsou upraveny nejdůležitější aspekty problematiky soukromí na pracovišti, potažmo kamerového a e-mailového monitoringu. Myslím, že právě finský zákon o ochraně soukromí v pracovním životě by mohl být pro českého zákonodárce inspirativním právním předpisem.

Uznávám, že přijetí a shoda na takovém právním předpisu bude složitá. Nelze totiž opomenout to, že při monitoringu zaměstnanců dochází často ke konfliktu mezi Listinou garantovaným právem zaměstnance a právem zaměstnavatele. Monitoring zaměstnanců je tedy typickým institutem, u kterého se setkáváme se střetem práva soukromého s právem veřejným. Není proto možné na monitoring nahlížet ryze z pohledu pracovního práva. Podíváme-li se zpět na nástin právních předpisů uvedený v 1. kapitole této diplomové práce, zjistíme, že pro komplexní pochopení této problematiky je na monitoring zaměstnanců nutné nahlížet též z pohledu práva unijního, práva občanského, práva správního, ale též z pohledu práva trestního. U neoprávněného monitoringu e-mailových stránek či firemních telefonů totiž zaměstnavatel může snadno svým jednáním naplnit skutkovou podstatu trestného činu porušení tajemství dopravovaných zpráv ve smyslu§ 182 zákona č. 40/2009 Sb., trestního zákoníku, v platném znění. Pokud pak zaměstnavatel nesplní svou informační povinnost o rozsahu a způsobech jím prováděné kontroly, může jeho jednání pro změnu naplnit skutkovou podstatu přestupku ve smyslu ust. § 11a či ust. §24a zákona č. 251/2005 Sb., o inspekci práce.

V diplomové práci jsem věnovala prostor také testování zaměstnanců, které bylo v roce 2021 diskutovaným a aktuálním tématem. Mnozí se domnívali, že sledování zdravotního stavu zaměstnanců prostřednictvím nařízeného testování je protiprávní. Po prostudování odborných článků a judikatury jsem však dospěla k závěru, že tyto názory nebyly správné. Lze proto očekávat, že bude-li zde v budoucnu pandemie tohoto či jiného infekčního onemocnění v obdobném

rozsahu, bude opět zaměstnavatelům uložena povinnost své zaměstnance pravidelně testovat.

Testování zaměstnanců na covid-19 není jedinou formou monitoringu, se kterou se můžeme setkat. Do budoucna se navíc dle mého názoru bude výčet forem monitoringu rozrůstat. U všech forem monitoringu lze zaměstnavatelům souhrnně doporučit, aby neopomíjeli, že každý monitoring je zásahem do soukromí zaměstnanců. Důrazně zaměstnavatelům doporučuji, ať pečlivě uváží, zda je zavedení monitoringu opravdu nezbytné. Díky monitoringu lze totiž velmi snadno pokazit náladu na pracovišti i ztratit důvěru svých zaměstnanců. Zohledňovány by tedy neměly být pouze zájmy ekonomické, ale též morální. I morální aspekt činí z monitoringu zaměstnanců zajímavé téma, a proto bych se i morálnímu aspektu tohoto institutu věnovala blíže a podrobněji v budoucnu.

Resumé

In my diploma thesis I focused on employee monitoring in the light of the case law of the Czech Republic. It is a very wide-ranging topic, which cannot be conceived thoroughly with regard to the scope of the thesis. In the beginning of this diploma thesis, I set myself the goal of providing a basic insight into the issue of employee monitoring, describing the current state and provide a comprehensive overview of selected forms of monitoring.

It is clear that the European Union is trying to respond to the employee monitoring and personal data processing trends, by adopting legal norms. The European Data Protection Board also plays a significant role in the monitoring and processing of employees' personal data. It is able to respond to the political and social issues much more flexibly (eg the Covid-19 pandemic) by adopting various legal instruments. However, a knowledge of the instruments above is among employers and employees, in my personal opinion, very low. I find this unfortunate, as I personally consider the European Data Protection Board documents to be an excellent tool for interpretation and application. For better understanding the issue, it is also important to work with case law. In my diploma thesis, I focused my attention on the most important case law related to the issue of employee monitoring. Although we do not yet find a large number of judgments in which Czech courts deal with employee monitoring, the case law of the European Court of Human Rights is, on the other hand, the main source. I am going to pay more attention to the case law of the ECtHR in my further research.

Modern technologies and trends in the human resources industry are constantly evolving. The Covid-19 pandemic and the current war in Ukraine demonstrate how vulnerable and dependent our economy is on the outside world. We are also following the rapid development in the field of modern technologies. Therefore, employers can be expected to look for other ways to monitor their employees and optimize their costs. In addition, with the development of technology, I anticipate that in the future, employees will need business phones, the Internet and other resources for their job much more than they do today. For the reasons set out above, I therefore presume that it is right that we have defined legislation in general sense. In my opinion, general legislation can respond better to developments and technological progress. Especially in our country, where the legislative process of passing laws is long.

However, I find it problematic that the employee monitoring legislation is fragmented among many pieces of legislation. It is necessary to assume that the addressees of legal norms are primarily lay people and the fragmentation of legal regulation makes it quite difficult for them to interpret and orient themselves correctly. I would therefore recommend the legislator to draw inspiration from the Finnish legislation here. Finland has embarked on a path of more comprehensive law, which regulates the most important aspects of workplace privacy, including camera and e-mail monitoring. I think that the Finnish law on the protection of privacy in working life could be an inspiring piece of legislation for the Czech legislator.

I admit that adopting and agreeing on such legislation will be difficult. It must not be forgotten that during the employee monitoring, there is often a conflict between the employee's right and the employer's right guaranteed by Charter of Fundamental Rights and Freedoms. Employee monitoring is therefore a typical institute where we encounter a conflict between private law and public law. It is therefore not possible to look at monitoring purely from the point of view of labor law. If we look back at the outline of legislation in Chapter 1 of this thesis, for a comprehensive understanding of this issue, we find that the employee monitoring must also be seen from the perspective of EU law, civil law, administrative law, but also criminal law. In the case of unauthorized monitoring of e-mail pages or business phones, the employer can easily fulfill the crime elements of violating the secrecy of transported messages within the meaning of Section 182 of Act No. 40/2009 Coll., The Criminal Code, as amended. If the employer then fails to fulfill its information obligation on the scope and methods of its inspection, its action for change may fulfill the crime elements of the transgression within the meaning of Section 11a or 24a of Act No. 251/2005 Coll., On Labor Inspection.

In my diploma thesis, I also devoted space to employee testing, which was a discussed and current topic in 2021. Many people thought that the employees‘ health mandatory testing was illegal. However, after studying the professional articles and case law, I came to a conclusion that these views were not correct. Therefore, it can be expected that if there is a pandemic of an infectious desease in the future, the employers will be required to retest their employees.

Testing employees at COVID-19 is not the only monitoring form we can encounter. In addition, in my opinion, the list of monitoring forms will grow in the future. For all monitoring forms, employers can be advised not to forget that any

monitoring is an intrusion on employees' privacy. I strongly encourage employers to carefully consider whether the initiation of monitoring is really necessary. Thanks to monitoring, it is very easy to spoil the workplace mood and lose the employees‘ trust. Therefore, not only economic interests but also moral interests should be taken into account. The moral aspect also makes employee monitoring an interesting topic, and therefore I would pay more attention to the moral aspect of this institute in the future.

Seznam použitých zdrojů

Prameny

České

Mimořádné opatření Ministerstva zdravotnictví č.j. MZDR 42085/2021-2/MIN/KAN.

Mimořádné opatření Ministerstva zdravotnictví MZDR 47828/2020-22/MIN/KAN.

Mimořádné opatření Ministerstva zdravotnictví MZDR 9364/2021-1/MIN/KAN.

Mimořádné opatření Ministerstva zdravotnictví ze dne 1. března 2021, č. j. MZDR 47828/2020-16/MIN/KAN.

Mimořádné opatření Ministerstva zdravotnictví ze dne 20. listopadu 2021, č. j. MZDR 42085/2021-1/MIN/KAN.

Nařízení vlády č. 168/2002 Sb., kterým se stanoví způsob organizace práce a pracovních postupů, které je zaměstnavatel povinen zajistit při provozování dopravy dopravními prostředky.

Sdělení č. 209/1992 Sb., Sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.

Usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 110/2019 Sb., zákon o zpracování osobních údajů, ve znění pozdějších předpisů.

Zákon č. 251/2005 Sb., o inspekci práce, ve znění pozdějších předpisů.

Zákon č. 255/2012 Sb., o kontrole, ve znění pozdějších předpisů.

Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

Zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů.

Zákon č. 361/2000 Sb., zákon o provozu na pozemních komunikacích a o změně některých zákonů, ve znění pozdějších předpisů.

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů.

Zákon č. 435/2004 Sb., zákon o zaměstnanosti, ve znění pozdějších předpisů.

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

Cizojazyčné

Federální zákon o ochraně údajů (org. *Bundesdatenschutzgesetz).*

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR).

Německý občanský zákoník (org. *Bürgerliches Gesetzbuch).*

Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

Základní zákon spolkové republiky Německo (org. *Grundgesetz für die Bundesrepublik Deutschland*).

Zákon o ochraně osobních údajů (*Data Protection Act (1050/2018), org. Tietosuojalaki/Dataskyddslag (1050/2018)*).

Zákon o ochraně soukromí v pracovním životě (*Act on the Protection of Privacy in Working*, org. *Laki yksityisyyden suojasta työelämässä* (13.8.2004/759).

Zákon o pracovních vztazích v podnicích (org. *Betriebsverfassungsgesetz).*

Zákon o telekomunikacích (org. *Telekommunikationgesetz).*

Zákon o telemédiích *(org. Telemediegesetz).*

Literatura

Česká

BĚLINA, M., DRÁPAL, L. a kol. *Zákoník práce*. 3. vydání. Praha: C. H. Beck, 2019, marg. č. 1.

LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. 2. vydání. Praha: C. H. Beck, 2022. marg. č. 36.

MORÁVEK J. (ed.). *Pracovní právo 2021: Sociální právo v době (post)covidové*. 1. vydání. Praha: Univerzita Karlova, Právnická fakulta, 2021. ISBN: 978-80-7630-016-3.

ŠÁMAL, P., NOVOTNÝ, O., GŘIVNA, T. a kol. *Trestní právo hmotné.* 8. přepracované vydání. Praha: Wolters Kluwer. 2016. ISBN 978-80-7552-358-7.

UŘIČAŘ, M., RÁMIŠ, V. a kol. *Obecné nařízení o ochraně osobních údajů.* 1. vydání. Praha: C. H. Beck, 2021.

VIDRNA, J., KOUDELKA, Z. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců*. V Praze: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7.

ZAHRADNÍČEK, J. *Ochrana osobnosti v pracovněprávních vztazích*. Praha: Leges, 2019. Teoretik. ISBN 978-80-7502-373-5.

Cizojazyčná

International Labour Office (ILO). *Code of Practice: Protection of Worker's personal data*.). Geneva: International Labour Office, 1997. Čl. 6.14. a násl. ISBN 92-2-110329-3. Online dostupný z: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/
safework/documents/normativeinstrument/wcms_107797.pdf.

Odborné články

České

BLAŽEK, V. Kritika zaměstnavatele na sociálních sítích jako důvod pro skončení pracovního poměru. *Epravo.cz.* [online]. Publikováno 7. 1. 2016 [cit. 31. 3. 2022].

Dostupné z: https://www.epravo.cz/top/clanky/kritika-zamestnavatele-na-socialnich-sitich-jako-duvod-pro-skonceni-pracovniho-pomeru-99663.html.

BURIAN, D., RADIČOVÁ Z. Mezinárodní předávání osobních údajů z pohledu nové regulace ochrany osobních údajů. *Právní prostor.* [online]. Publikováno 13. 4. 2016 [cit. 31. 3. 2022]. Dostupné z: https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/mezinarodni-predavani-osobnich-udaju-z-pohledu-nove-regulace-ochrany-osobnich-udaju.

FIALOVÁ, E. Ochrana soukromí ve světle judikatury Evropského soudu pro lidská práva. *Časopis pro právní vědu a praxi.* [online]. Publikováno 3. 9. 2012, č. 20(2), s. 123 [cit. 31. 3. 2022]. ISSN 1805-2789. Dostupné z: https://journals.muni.cz/cpvp/article/view/5875/4982.

GORČÍK, J. Porušení povinností zaměstnance ve světle judikatury Nejvyššího soudu aneb šance pro zaměstnavatele při sporech se zaměstnanci. *Právní prostor.* [online]. Publikováno 1. 10. 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/poruseni-povinnosti-zamestnance-ve-svetle-judikatury-nejvyssiho-soudu-aneb-sance-pro-zamestnavatele-pri-sporech-se-zamestnanci.

JOUZA, L. Ochrana osobnosti zaměstnance v pracovněprávních vztazích. *Bulletin advokacie*. 2014, č. 6, s. 29. ISSN 1210-6348.

KADLECOVÁ, T. GPS ve služebních vozidlech aneb malý čip = velká komplikace?. *Praktická personalistika*. Sagit, 2015, 2015(3-4/2015).

LUPIENSKÁ, P. Docházkový systém s použitím biometriky - otisk prstů zaměstnanců. Co na to GDPR?. *Právní prostor.* [online]. Publikováno 17. 3. 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.pravniprostor.cz/clanky/spravni-pravo/dochazkovy-system-s-pouzitim-biometriky-otisky-prstu-zamestnancu-co-na-to-gdpr?.

MORÁVEK, J. Kontrola a sledování zaměstnanců – výklad § 316 ZPr. *Právní rozhledy*, 2017, č. 17.

MURAD, M., UHRINOVÁ, A. Monitoring činností zaměstnanců ze strany zaměstnavatele (1. část). *Epravo.cz.* [online]. Publikováno 25. 6. 2019 [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/monitoring-cinnosti-zamestnancu-ze-strany-zamestnavatele-1-cast-109563.html.

NONNEMANN, F. Vztahuje se GDPR i na online kamery?. *Epravo.cz.* [online]. Publikováno 2. 3. 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/vztahuje-se-gdpr-i-na-online-kamery-110746.html.

ODROBINOVÁ, V. Nařízené testování zaměstnanců z pohledu GDPR. *Práce a mzda.* [online]. Publikováno 22. 10. 2021. [cit. 31. 3. 2022]. Dostupné z: https://www.praceamzda.cz/clanky/narizene-testovani-zamestnancu-z-pohledu-gdpr.

PEJCHALOVÁ GRÜNWALDOVÁ, V. Evropský soud pro lidská práva: K zásahu do soukromí zaměstnanců. *Advokátní deník.* [online]. Publikováno 19. 3. 2020 [cit. 31. 3. 2022]. Dostupné z: https://advokatnidenik.cz/2020/03/19/evropsky-soud-pro-lidska-prava-k-zasahu-do-soukromi-zamestnancu.

POMAIZLOVÁ, K., DOLEŽAL, R. Monitoring emailových zpráv zaměstnanců. *Epravo.cz* [online]. Publikováno 23. 3. 2021 [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/monitoring-emailovych-zprav-zamestnancu-112690.html.

PRAVDOVÁ, M. Sociální média na pracovišti. *Právní prostor.* [online]. Publikováno 21. 5. 2018. [cit. 31. 3. 2022]. Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/socialni-media-na-pracovisti.

PROCHÁZKOVÁ, E. Několik poznámek k monitoringu zaměstnanců. *Epravo.cz.* [online]. Publikováno 11. 10. 2017 [cit. 2022-03-23]. Dostupné z: https://www.epravo.cz/top/clanky/nekolik-poznamek-k-monitoringu-zamestnancu-106512.html.

PROUZA, J. Zpracování biometrických údajů zaměstnanců. *Epravo.cz.* [online]. Publikováno 22. 8. 2019. [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-zamestnancu-109845.html.

RADIČOVÁ, Z. Monitoring zaměstnanců prostřednictvím GPS technologie. *Právní rozhledy*, 2014, č. 21, s. 736-740.

UHRINOVÁ, A., MENZELOVÁ K. *Vybrané způsoby monitoringu zaměstnance pracujícího z domova a jejich právní mantinely.* In.: MORÁVEK J. (ed.). *Pracovní právo 2021: Sociální právo v době (post)covidové*. 1. vydání. Praha: Univerzita

Karlova, Právnická fakulta, 2021. s. 85-105. ISBN: 978-80-7630-016-3. Online dostupné z: https://rozkotova.cld.bz/Pracovni-pravo-2021?fbclid=IwAR1kY.

VALIŠOVÁ, V. K otázce interních předpisů zaměstnavatele ve vztahu k prevenci onemocnění covid-19 v otázkách a odpovědích. *Advokátní deník.* [online]. Publikováno 10. 9. 2021. [cit. 31. 3. 2022]. Dostupné z: https://advokatnidenik.cz/2021/09/10/k-otazce-internich-predpisu-zamestnavatele-ve-vztahu-k-prevenci-onemocneni-covid-19-v-otazkach-a-odpovedich/.

VRBÍKOVÁ, B. Stanovisko Pracovní skupiny 29 k monitorování zaměstnanců na pracovišti i mimo něj. *Epravo.cz.* [online]. Publikováno 13. 9. 2017. [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/stanovisko-pracovni-skupiny-29-k-monitorovani-zamestnancu-na-pracovisti-i-mimo-nej-106342.html.

ZEMANOVÁ ŠIMONOVÁ, H. Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů. *Bulletin advokacie*. 2017, č. 9. s. 25-32. ISSN 1210-6348.

ZVOLÁNEK, J., MALATINCOVÁ, D. Může si zaměstnavatel přečíst e-maily bývalého zaměstnance?. *Epravo.cz.* [online]. Publikováno 15. 7. 2020 [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/muze-si-zamestnavatel-precist-e-maily-byvaleho-zamestnance-111482.html.

Cizojazyčné

EKLUND, M. C. Monitoring employees' e-mail correspondence and Internet use – A Finnish perspective – PART I. *European Labour Law Journal*, 2019, 10(2), s. 116–133. DOI: 10.1177/2031952519852110.

WARREN, S. D., BRANEIS, L. D. The Right to Privacy *The Harward Law Review.* [online]. 1890, roč. 4, č. [cit. 31. 3. 2022]. Dostupné z: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.

Judikatura

Česká

Nález Ústavního soudu ze dne 12. 10. 1994, sp. zn. Pl. ÚS 4/94.

Nález Ústavního soudu ze dne 9. prosince 2014, sp. zn. II. ÚS 1774/14.

Rozhodnutí Nejvyššího soudu ze dne 16. 8. 2012, sp. zn. 21 Cdo 1771/2011.

Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 3. července 2013, sp. zn. UOOU-00237/13.

Rozsudek Městského soudu v Praze ze dne 18. 10. 2016, sp. zn. 5 A 107/2013.

Rozsudek Městského soudu v Praze ze dne 5. 5. 2017, sp. zn. 6 A 42/2013.

Rozsudek Nejvyššího soudu ze dne 11. 5. 2005, sp. zn. 30 Cdo 64/2004.

Rozsudek Nejvyššího soudu ze dne 20. 3. 2017, sp. zn. 21 Cdo 1043/2016.

Rozsudek Nejvyššího soudu ze dne 26. 7. 2000, sp. zn. 30 Cdo 2304/99.

Rozsudek Nejvyššího soudu ze dne 7. 8. 2014, sp. zn. 21 Cdo 747/2013.

Rozsudek Nejvyššího správního soudu ze dne 14. 4. 2021, sp. zn. 8 Ao 1/2021.

Rozsudek Nejvyššího správního soudu ze dne 20. 12. 2017, sp. zn. 10 As 245/2016.

Rozsudek Nejvyššího správního soudu ze dne 23. 8. 2013, sp. zn. 5 As 158/2012.

Rozsudek Nejvyššího správního soudu ze dne 4. 3. 2022, sp. zn. 5 Ao 31/2021.

Rozsudek Okresního soudu v Mělníku ze dne 11. 2. 2021, sp. zn. 6 C 306/2019.

Usnesení Ústavního soudu ze dne 31. 3. 2009, sp. zn. I. ÚS 452/09.

Usnesení Ústavního soudu ze dne 8. 1. 2019, sp. zn. I. ÚS 3900/18.

Usnesení Ústavního soudu ze dne 16. 8. 2017, sp. zn I. ÚS 1716/17.

Cizojazyčná

Rozhodnutí Evropského soudu pro lidská práva ze dne 26. 7. 2007, stížnost č. 64209/01 Peev proti Bulharsku.

Rozhodnutí Evropského soudu pro lidská práva ze 17. 7. 2003, stížnost č. č. 63737/00 Perry proti Spojenému království.

Rozhodnutí Federálního pracovního soudu (org. *Bundesarbeitsgericht)*) ze dne 27. 7. 2017, sp. zn. 2 AZR 681/16.

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

Rozhodnutí Federálního pracovního soudu ze dne 29. 6. 2004, sp. zn. 1 ABR 21/03.

Rozsudek Evropského soudu pro lidská práva ze dne 12. 1. 2016, stížnost č. 61496/08 Bărbulescu proti Rumunsku.

Rozsudek Evropského soudu pro lidská práva ze dne 16. 12. 1992, stížnost č. 13710/88 Niemitz versus Německo.

Rozsudek Evropského soudu pro lidská práva ze dne 25. 6. 1997, stížnost č. 20605/92 Halford proti Spojenému království.

Rozsudek Evropského soudu pro lidská práva ze dne 25. 9. 2001, stížnost č. 44787/98, P. G. a J. H. proti Spojenému království.

Rozsudek Evropského soudu pro lidská práva ze dne 3. 4. 2007, stížnost č. 62617/00 Coplandová proti Spojenému království.

Rozsudek Evropského soudu pro lidská práva ze dne 5. 9. 2017, stížnost č. 61496/08 Bărbulescu proti Rumunsku.

Rozsudek Evropského soudu pro lidská práva, stížnost č. 1874/13 a 8567/13 Lopéz Ribalda a ostatní proti Španělsku.

Rozsudek Federálního pracovního soudu ze dne 21. 11. 2013, sp. zn. 2 AZR 797/11.

Rozsudek Federálního pracovního soudu ze dne 21. 6. 2012, sp. zn. 2 AZR 153/11.

Rozsudek Státního pracovního soudu Berlín – Branderburg ze dne 14. 1. 2016, sp. zn. 5 So 657/15.

Jiné zdroje

České

ČT 24. *Za prací dojíždí do ciziny přes 56 tisíc Čechů. Nejvíc do Německa, míří ale i do Británie.* [online]. Publikováno 2. 9. 2019. [cit. 31. 3. 2022]. Dostupné z: https://ct24.ceskatelevize.cz/ekonomika/2912609-za-praci-dojizdi-do-ciziny-pres-56-tisic-cechu-nejvic-do-nemecka-miri-ale-i-do.

ePrávo.cz. *Zpracování osobních údajů zaměstnanců s přihlédnutím k možnosti sledování produktivity*. [online]. Publikováno 27. 8. 2018. [cit. 31. 3. 2022]. Dostupné z: https://www.epravo.cz/top/clanky/zpracovani-osobnich-udaju-zamestnancu-s-prihlednutim-k-moznosti-sledovani-produktivity-108065.html.

Ministerstvo zdravotnictví České republiky. *Mimořádné opatření*. [online]. Publikováno 22. 11. 2020. [cit. 31. 3. 2022] Dostupné z: https://www.mzcr.cz/wp-

content/uploads/2021/11/Zmena-mimoradneho-opatreni-ze-dne-20-11-2021-k-testovani-zamestnancu-a-osob-samostatne-vydelecne-cinnych-s-ucinnosti-od-23-11-2021.pdf.

Ministerstvo zdravotnictví České republiky. *Mimořádné opatření*. [online]. Publikováno 1. 3. 2020. [cit. 31. 3. 2022] Dostupné z: https://www.mzcr.cz/wp-content/uploads/2021/03/Mimoradne-opatreni-povinne-testovani-zamestnavatele-s-ucinnosti-od-3-3-2021-do-odvolani.pdf.

Novinky.cz. *Jak se měnil internet v Česku*. [online]. Publikováno 14. 2. 2017. [cit. 31. 3. 2022]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/prehledne-jak-se-menil-internet-v-cesku-40024418.

Novinky.cz. *Muž zmlátil ochrankáře, který ho nechtěl pustit do obchodu bez respirátoru.* [online]. Publikováno 11. 1. 2022. [cit. 31. 3. 2022]. Dostupné z: https://www.novinky.cz/krimi/clanek/muz-zmlatil-ochrankare-ktery-ho-nechtel-pustit-do-obchodu-bez-respiratoru-40383575.

Protokol o kontrole ÚOOÚ ze dne 9. ledna 2019, č.j. UOOU-09072/18-14.

Stanovisko ÚOOÚ č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. Dostupné z: https://www.uoou.cz/files/stanovisko_2009_2.pdf.

Stanovisko ÚOOÚ č. 6/2009: Ochrana soukromí při zpracování osobních údajů. Listopad 2009, aktualizace. Dostupné z: https://www.uoou.cz/files/stanovisko_2009_6.pdf.

Stanovisko ÚOOÚ č. 6/2012: Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů.

Státní úřad inspekce práce. *Monitorování zaměstnanců na pracovišti kamerovým systémem. Otázky a odpovědi*. [online]. Publikováno 7. 4. 2014 [cit. 31. 3. 2022]. Dostupné z: http://www.suip.cz/otazky-a-odpovedi/pracovnepravni-vztahy/ochrana-majetkovych-zajmu-zamestnavatele-a-ochrana-osobnich-prav-zamestnance/monitorovani-zamestnancu-na-pracovisti-kamerovym-systemem-pridano-7-14-2014/.

Státní úřad inspekce práce. *Podání podnětu*. [online]. Publikováno © 2022. [cit. 31. 3. 2022]. Dostupné z: http://epp.suip.cz/epp/index_light.php.

ÚOOÚ: Připomínka k návrhu zákona, kterým se mění zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů a zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů.

ÚOOÚ: Stanovisko č. 1/2006: Provozování kamerového systému z hlediska zákona o ochraně osobních údajů. Leden 2006.

ÚOOÚ: Stanovisko č. 5/2013: Pořizování hlasových záznamů v rámci elektronické komunikace při poskytování služeb z pohledu zákona o ochraně osobních údajů. Říjen 2013.

Úřad pro ochranu osobních údajů. *K povinnému testování zaměstnanců – rozšířené vyjádření.* [online]. Změněno 26. 3. 2021. [cit. 31. 3. 2022] Dostupné z: https://www.uoou.cz/k-povinnemu-testovani-zamestnancu-rozsirene-vyjadreni/d-48835.

Úřad pro ochranu osobních údajů. *K provozování kamerových systémů*. Nejčastější otázky a odpovědi. [online]. © 2013 [cit. 31. 3. 2022]. Dostupné z: https://www.uoou.cz/k-provozovani-kamerovych-systemu/d-29535.

Úřad pro ochranu osobních údajů. *Připomínka, č.j. UOOU-02950/19-4.* [online]. Publikováno 29. 7. 2019. [cit. 31. 3. 2022]. Dostupné z: Návrh ke změně zákona dostupný zde: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=35418.

Úřad pro ochranu osobních údajů. *Rozhodnutí předsedy úřadu*. [online]. © 2013[cit. 31. 3. 2022]. Dostupné z: https://www.uoou.cz/rozhodnuti-predsedy-uradu/ds-3815

Úřad pro ochranu osobních údajů. *Stanovisko č. 1/2010 ÚOOÚ: Služby soukromých detektivů z pohledu ochrany osobních údajů*. [online]. Aktualizováno srpen 2010. [cit. 31. 3. 2022] Dostupné z: https://www.uoou.cz/files/stanovisko_2010_1.pdf.

Úřad pro ochranu osobních údajů. *ÚOOÚ navrhuje změny v oblasti zpracování biometrických údajů zaměstnanců.* [online]. Publikováno 30. 7. 2019. [cit. 31. 3. 2022]. Dostupné z: https://www.uoou.cz/uoou-navrhuje-zmeny-v-oblasti-zpracovani-biometrickych-udaju-zamestnancu/d-35406.

Cizojazyčné

BBC. *Ikea France fined €1m for snooping on staff*. [online]. Publikováno 15. 6. 2021 [cit. 31. 3. 2022]. Dostupné z: https://www.bbc.com/news/world-europe-57482168.

Bundesministerium der Justiz. Bundesamt für Justiz. *Grundgesetz für die Bundesrepubklik Deutschland.* [online]. Změněno 29. 9. 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.gesetze-im-internet.de/gg/BJNR000010949.html.

Bundesministerium der Justiz. Bundesamt für Justiz. *Telekommunikationgesetz.* [online]. Publikováno 23. 6. 2021. [cit. 31. 3. 2022]. Dostupné z: https://www.gesetze-im-internet.de/tkg_2021/.

Bundesministerium der Justiz. Bundesamt für Justiz. *Telemediegesetz.* [online]. Publikováno 26. 2. 2007. [cit. 31. 3. 2022]. Dostupné z: https://www.gesetze-im-internet.de/tmg/.

Doporučení č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad s úrovní ochrany osobních údajů v EU.

European Data Protection Board. *Prohlášení o zpracování osobních údajů v souvislosti s výskytem onemocnění covid-19.* [online]. Publikováno 11. 3. 2020. [cit. 31. 3. 2022]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_art_23gdpr_20200602_cs_1.pdf.

Europion Data Protection Board. *Doporučení č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soudlad s úrovní ochrany osobních údajů v EU.* [online]. Přijato 10. 11. 2020 [cit. 31. 3. 2022]. https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_cs.pdf.

FinLex. *1050/2018.* [online]. Publikováno 5. 12. 2018. [cit. 31. 3. 2022]. Dostupné z: https://www.finlex.fi/fi/laki/alkup/2018/20181050.

FinLex. *13.8.2004/759.* [online]. Publikováno 13. 8. 2004. [cit. 31. 3. 2022]. Dostupné z: https://www.finlex.fi/fi/laki/ajantasa/2004/20040759.
Anglický překlad dostupný z:https://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf.

GSK. *GSK Public Statements*. [online]. Publikováno prosinec 2020. [cit. 31. 3. 2022]. Dostupné z: https://www.gsk.com/media/6870/czech.pdf.

KONE.com. *Etický kodex společnosti KONE*. [online]. Publikováno září 2021 [cit. 31. 3. 2022]. Dostupné z: https://www.kone.com/fi/Images/KONE-Code-of-Conduct-Czech_tcm18-68547.pdf.

MÖLLER, F. *Video surveillance of employees in Germany: get ready for compliance checks!*. Ius Laboris. [online]. Publikováno 11. 3. 2021. [cit. 31. 3. 2022]. Dostupné z: https://iuslaboris.com/insights/video-surveillance-of-employees-in-germany-get-ready-for-compliance-checks/?.

Pokyn Evropského sboru pro ochranu osobních údajů č. 01/2020 ke zpracování osobních údajů v souvislosti s propojenými vozidly a aplikacemi souvisejícími s mobilitou, verze 2.0. (v originále: *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*) ze dne 9. března 2021.

Pokyn Evropského sboru pro ochranu osobních údajů č. 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky, verze 2.0. (v originále: *Guidelines 3/2019 on processing of personal data through video devices*) ze dne 29. ledna 2020.

Pracovní dokument WP29: Ke sledování elektronických komunikací na pracovišti (v originále: *Working document on the surveillance of electronic communications in the workplace*) ze dne 29. května 2002.

PRESTEL, Patrick a Max-Lion KELLER. Überwachung und Kontrolle des Arbeitnehmers und die Konflikte mit dem Fernmeldegeheimnis und dem Datenschutz (7. Teil der neuen Serie der IT-Recht Kanzlei zu den Themen E-Mailarchivierung und IT-Richtlinie). *It-recht kanzlei München.* [online]. Publikováno 6. 7. 2010. [cit. 31. 3. 2022]. Dostupné z: https://www.it-recht-kanzlei.de/e-mail-archivierung-%C3%BCberwachung-kontrolle-arbeitnehmer-fernmeldegeheimnis-datenschutz.html.

Prováděcí rozhodnutí Komise ze dne 19. prosince 2012 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů na Novém Zélandu.

Prováděcí rozhodnutí Komise ze dne 23. ledna 2019 podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající ochraně osobních údajů poskytované Japonskem na základě zákona o ochraně osobních informací.

Rozhodnutí Komise ze dne 31. ledna 2011 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů státem Izrael v souvislosti s automatizovaným zpracováním osobních údajů.

Seznam zemí zařazených do EHP je k dispozici například zde: https://www.kb.cz/getmedia/6ac33196-62a7-423b-8841-667680dfa6ff/Seznam-Zemi-EU-EHP-SEPA.pdf.aspx.

Shell.cz. *Shell privacy rulles.* [online]. Publikováno 20. 5. 2019 [cit. 31. 3. 2022]. Dostupné z: https://www.shell.cz/privacy/_jcr_content/par/textimage_68bd.stream/1582033078118/cbd1d82ecc649f343df1032f40f8c661baf6d647/shell-binding-corporate-rules.pdf.

Stanovisko WP29 č. 2/2017: ke zpracování osobních údajů na pracovišti (v originále: *Opinion 2/2017 on data processing at work*) ze dne 8. června 2017.

Stanovisko WP29 č. 4/2004: Ke zpracování osobních údajů prostředky kamerového sledování (11750/02/EN/WP89) (v originále: *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*) ze dne 11. února 2004, s. 3, dostupné na: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf.

Stanovisko WP29 č. 5/2005: K užívání lokačních údajů s přihlédnutím k poskytování služeb s přidanou hodnotou. (v originále: *Opinion on the use of location data with a view to providing value-added services*) ze dne 25. listopadu 2005.

Stanovisko WP29 č. 8/2001: Zpracování osobních údajů v kontextu zaměstnání.

Tietosuojavaltuutetun Toimisto. *Oikopolkuja.* [online]. Publikováno © 2022. [cit. 31. 3. 2022]. Dostupné z: https://tietosuoja.fi.