EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja

OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.

2023

Právo na ochranu osobného súkromia a ochrana osobných údajov v pracovnoprávnych vzťahoch

NÁRODNÝ PROJEKT

Podpora kvality sociálneho dialógu

Typ projektu: Neinvestičný

Termín realizácie projektu: 07/2018 – 11/2023

ITMS projektu: 312031V749

Autorský kolektív :

prof. JUDr. Juraj Hamuľák, PhD.

doc. JUDr. Matej Horvat, PhD.

JUDr. Andrej Poruban, PhD.

JUDr. Jozef Greguš, PhD., LL.M.

JUDr. Matúš Mesarčík, PhD., LL.M.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Autorské dielo bolo vypracované v rámci hlavnej aktivity „Posilnenie odborných a analytických kapacít sociálnych partnerov, budovanie infraštruktúry a komunikačnej platformy sociálneho dialógu a rozvoja sociálneho partnerstva na národnej a medzinárodnej úrovni“ v rámci podaktivity 1.1 Posilnenie kapacít sociálnych partnerov prostredníctvom analytickej činnosti Národného projektu Podpora kvality sociálneho dialógu expertným tímom sociálneho partnera - štát. Vyjadruje názory a postoje sociálneho partnera na predmetnú tému. Autorské dielo nevyjadruje názory ani postoje prijímateľa projektu a bolo schválené Riadiacim výborom Národného projektu Podpora kvality sociálneho dialógu.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Obsah

ÚVOD 10
1 SOCIÁLNE PRÁVA – TEORETICKÉ VYMEDZENIE 11
1.1 PRÁVO NA OCHRANU OSOBNÝCH ÚDAJOV A SÚKROMIA V SYSTEMATIKE ĽUDSKÝCH PRÁV 11
1.2 AUTONÓMIA A SÚKROMIE JEDNOTLIVCA 12
1.2.1 Subjekty individuálnych pracovnoprávnych vzťahov 13
1.2.1.1 Zamestnávateľ 13
1.2.1.2 Zamestnanec 15
1.2.2 Autonómia jednotlivca a zásada zmluvnosti 17
1.3 PRAMENE PRÁVA UPRAVUJÚCE OCHRANU OSOBNÝCH ÚDAJOV A SÚKROMIA 19
1.3.1 Všeobecne k prameňom práva 19
1.4 DRUHY PRAMEŇOV PRACOVNÉHO PRÁVA 20
1.4.1 Európske pramene 20
1.4.2 Vnútroštátne pramene 22
1.4.3 Právna úprava ochrany súkromia v pracovnoprávnych predpisoch 23
2 OCHRANA OSOBNÝCH ÚDAJOV ZAMESTNANCA PODĽA NARIADENIA GDPR 33
2.1 SUBJEKTY PARTICIPUJÚCE V SYSTÉME OCHRANY OSOBNÝCH ÚDAJOV 35
2.1.1 Prevádzkovateľ 36
2.1.2 Spoloční prevádzkovatelia 39
2.1.3 Sprostredkovateľ 39
2.1.4 Iné subjekty 40
2.1.4.1 Zamestnanci ako dotknuté osoby 41
2.1.5 Špecifické subjekty 42
2.1.5.1 Oprávnená osoba 42
2.1.5.2 Zodpovedná osoba (DPO) 42
2.2 VYBRANÉ PRÁVA A POVINNOSTI ZAMESTNÁVATEĽA Z POHĽADU OCHRANY OSOBNÝCH ÚDAJOV 45
2.2.1 Základné zásady spracúvania osobných údajov z pohľadu zamestnávateľa 46
2.2.1.1 Zásada zákonnosti (spravodlivosti a transparentnosti) 47
2.2.1.2 Zásada obmedzenia účelu 48
2.2.1.3 Zásada minimalizácie údajov 50
2.2.1.4 Zásada správnosti 51

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2.2.1.5 Zásada minimalizácie uchovávania údajov 52
2.2.1.6 Zásada integrity a dôvernosti (bezpečnosť) 52
2.2.1.7 Zásada zodpovednosti 54
2.2.2 Posúdenie vplyvu na ochranu údajov a pracovnoprávne vzťahy 55
2.2.3 Súhlas a iné právne základy spracúvania osobných údajov v kontexte pracovnoprávnych vzťahov 60
2.2.3.1 Súhlas 62
2.2.3.2 Plnenie zmluvy 66
2.2.3.3 Zákonná povinnosť 67
2.2.3.4 Životne dôležitý záujem 68
2.2.3.5 Verejný záujem 68
2.2.3.6 Oprávnený záujem 69
3 OCHRANA OSOBNÝCH ÚDAJOV ZAMESTNANCA PODĽA ZÁKONA O OCHRANE OSOBNÝCH ÚDAJOV 75
3.1 VZÁJOMNÉ INTERAKCIE MEDZI ZÁKONOM O OCHRANE OSOBNÝCH ÚDAJOV A GDPR 75
3.1.1 Otvorené klauzuly 76
3.1.1.1 Derogácia GDPR podľa článku 23 GDPR 79
3.1.1.2 Samoregulačné nástroje 80
3.2 APLIKAČNÉ PROBLÉMY 81
3.3 NÁVRHY DE LEGE FERENDA 89
4 OCHRANA OSOBNÝCH ÚDAJOV A SÚKROMIA ZAMESTNANCA V PREDZMLUVNÝCH VZŤAHOCH 92
4.1 PRÁVO NA PRÍSTUP K ZAMESTNANIU 92
4.2 UCHÁDZAČ O ZAMESTNANIE A OCHRANA OSOBNÝCH ÚDAJOV 93
4.2.1 Uchádzač o zamestnanie v zmysle zákona o službách zamestnanosti 93
4.2.2 Záujemca o zamestnanie 94
4.2.3 Znevýhodnený uchádzač o zamestnanie 94
4.3 UCHÁDZAČ O ZAMESTNANIE A PREDZMLUVNÉ PRACOVNOPRÁVNE VZŤAHY 95
4.3.1 Zákaz zamestnávateľa vyžadovať určité informácie 97
4.3.2 Informačné povinnosti fyzickej osoby – budúceho zamestnanca 98
5 NEZÁKONNÉ ZÁSAHY DO OCHRANY SÚKROMIA ZAMESTNANCOV 100
5.1 MONITOROVANIE PRED A PO SKONČENÍ PRACOVNOPRÁVNEHO VZŤAHU 100
5.2 SUBJEKTY MONITORUJÚCE ZAMESTNANCOV 102

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

5.3 MONITOROVANIE E-MAILOVEJ KOMUNIKÁCIE ... 103
5.4 KONTROLA NA PRACOVISKU POMOCOU VIDEOKAMIER ALEBO MIKROFÓNOV ... 105
5.5 KONTROLA PROSTREDNÍCTVOM BIOMETRICKÝCH ÚDAJOV ... 106
5.6 MYSTERRY SHOPPING ... 110
5.7 NOVÉ TRENDY V OBLASTI MONITOROVANIA ZAMESTNANCOV ... 114
5.7.1 Kontrola e-mailovej komunikácie zamestnanca ... 116
5.7.2 Monitorovanie internetových stránok a mobilných aplikácií ... 117
5.7.3 Monitorovanie zamestnancov GPS systémom ... 119
5.7.3.1 Charakteristika GPS systému ... 119
5.7.3.2 Podmienky monitorovania zamestnancov ... 119
5.7.3.3 Pracovisko zamestnanca ... 120
5.7.4 Mobilný zamestnanec v cestnej doprave ... 121
5.7.4.1 Informačná povinnosť zamestnávateľa a súhlas zamestnanca ... 123
5.7.5 Právo zamestnanca odpojiť sa ... 125
5.8 KONTROLA VECÍ ... 126
5.9 OSOBNÝ SPIS ... 129
5.9.1 Forma a obsah osobného spisu ... 131
5.9.2 Právo zamestnanca na prístup k údajom, ktoré sa ho týkajú ... 133
5.9.3 Právo nahliadnuť do osobného spisu podľa ZP ... 134
5.9.4 Právo na prístup k údajom podľa GDPR ... 138
5.10 PREDKLADANIE SPRÁV O DOHODNUTÝCH NOVÝCH PRACOVNÝCH POMEROCH ... 141
6 VÝNIMKY ZO ZÁSAHOV DO OCHRANY SÚKROMIA ZAMESTNANCOV ... 143
6.1 KRITÉRIUM LEGALITY ... 145
6.2 KRITÉRIUM LEGITIMITY ... 146
6.3 KRITÉRIUM PROPORCIONALITY ... 147
6.4 POSÚDENIE VÝNIMKY SÚDOM ... 148
7 ROZHODOVACIA ČINNOSŤ NAJVYŠŠÍCH SÚDNYCH AUTORÍT ... 150
7.1 PRÁVO NA SÚKROMIE ... 150
7.2 JUDIKATÚRA ESĽP SÚVISIACA S OCHRANOU OSOBNÝCH ÚDAJOV ... 152
7.2.1 Rozhodovacia činnosť ESĽP a osobné údaje ... 152
7.3 VŠEOBECNE K ROZHODOVACEJ ČINNOSTI SÚVISIACEJ SO ZAMESTNANECKÝMI VZŤAHMI ... 160
7.3.1 Operácie s údajmi, ktoré môžu porušiť právo na rešpektovanie súkromného života – zhromažďovanie osobných údajov ... 163
7.3.1.1 Zber údajov zamestnávateľmi na pracovisku ... 163
7.3.1.2 Uchovávanie osobných údajov ... 168

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

7.3.1.3 Zverejnenie osobných údajov 169
7.3.1.4 Vplyv predchádzajúceho súhlasu 170
7.3.2 Ochrana osobných údajov v kontexte práva na spravodlivý proces 171
7.3.2.1 Rovnosť zbraní a rešpektovanie zásady kontradiktórnosti v konaniach týkajúcich sa citlivých alebo dôverných informácií 172
7.3.2.2 Zdôvodňovanie súdnych rozhodnutí a ochrana údajov 172
7.3.2.3 Použitie osobných údajov zhromaždených nezákonne alebo v rozpore s článkom 8 Dohovoru ako dôkazu 173
7.3.2.4 Dĺžka súdnych konaní týkajúcich sa ochrany údajov 173
7.3.2.5 Právo na účinný prostriedok nápravy (článok 13 Dohovoru) 174
7.3.3 Vybrané rozhodnutia ESĽP – bližšie vymedzenie prípadov a ich zhrnutia 175
7.3.3.1 GPS dáta 175
7.3.3.2 Monitorovanie používania počítača zamestnancami 176
7.3.3.3 Video dohľad 177
7.3.3.4 Trestnoprávny kontext 179
7.3.3.5 Uchovávanie v tajných registroch 180
7.3.3.6 Zverejnenie osobných údajov 180
7.4 ROZHODOVACIA ČINNOSŤ SÚDNEHO DVORA EÚ 181
7.4.1 Získavanie údajov o pracovnom príjme jednotlivca 181
7.4.2 Záznamy o pracovnom čase, zásady týkajúce sa kvality údajov a zákonnosti spracúvania údajov 183
7.5 HLBŠIA ANALÝZA VYBRANÝCH ROZHODNUTÍ ESĽP 183
7.5.1 Antović a Mirković vs. Čierna Hora - skutkové okolnosti prípadu 183
7.5.1.1 Analýza rozhodnutia ESĽP vo veci Antović a Mirković vs. Čierna Hora 186
7.5.1.2 Záverečné zhrnutie 192
7.5.2 Monitoring elektronickej komunikácie zamestnanca – prípad Barbulescu vs. Rumunsko 193
7.5.2.1 Právo na ochranu súkromia 193
7.5.2.2 Analýza jednotlivých rozhodnutí v prípade Barbulescu vs. Rumunsko 199
7.5.2.3 Prvé rozhodnutie 199

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

7.5.2.4 Rozhodnutie pred Veľkou komorou a rozhodnutie zo dňa 5.9.2017 202
7.5.2.5 Prípad Barbulescu v judikatúre Najvyššieho súdu Slovenskej republiky 204

8 PRÁVNE PROSTRIEDKY OCHRANY PRED NEZÁKONNÝM ZÁSAHOM DO SÚKROMIA ZAMESTNANCA 206

8.1 VŠEOBECNÉ VYMEDZENIE PRACOVNOPRÁVNYCH SPOROV 206
8.2 PRÁVNA OCHRANA PROSTREDNÍCTVOM ZAMESTNÁVATEĽA 208
8.3 PRÁVNA OCHRANA PROSTREDNÍCTVOM ZÁSTUPCOV ZAMESTNANCOV 212
8.4 PRÁVNA OCHRANA PROSTREDNÍCTVOM ORGÁNOV VEREJNEJ SPRÁVY 214
8.4.1 Národný inšpektorát práce a inšpektoráty práce 215
8.4.2 Úrad na ochranu osobných údajov 217
8.4.3 Úrad na ochranu oznamovateľov protispoločenskej činnosti 220
8.4.3.1 Pojem whistleblowing 221
8.4.3.2 Právna úprava whistleblowingu 222
8.4.3.3 Protispoločenská činnosť v pracovnoprávnych vzťahoch 222
8.4.3.4 Pozastavenie účinnosti právneho úkonu 223
8.4.3.5 Súhlas s pracovnoprávny úkonom 225
8.4.4 Slovenské národné stredisko pre ľudské práva 227
8.4.5 Verejný ochranca práv 229
8.4.6 Právna ochrana prostredníctvom mediátora 230
8.4.7 Právna ochrana prostredníctvom súdu 232

9 OCHRANA SÚKROMIA OSOBITNÝCH KATEGÓRII ZAMESTNANCOV 235

9.1 OCHRANA SÚKROMIA PROFESIONÁLNYCH ŠPORTOVCOV 235
9.2 OCHRANA SÚKROMIA PROFESIONÁLNYCH VODIČOV 239
9.2.1 Spôsoby a dôvody monitorovania zamestnancov v cestnej doprave 240
9.2.2 Monitorovanie GPS systémom 241
9.2.3 Informatívny merač rýchlosti 246
9.2.4 Ďalšie spôsoby monitorovania zamestnancov v cestnej doprave 247
9.2.5 Verejný záujem 251
9.3 OCHRANA SÚKROMIA SUDCOV 252
9.4 ZÁKON O SLOBODNOM PRÍSTUPE K INFORMÁCIÁM A OCHRANA OSOBNÝCH ÚDAJOV ZAMESTNANCOV ORGÁNOV VEREJNEJ MOCI (POVINNÝCH OSÔB) 257
9.4.1 Princípy infozákona 258
9.4.2 Vymedzenie pojmu informácia a povinnej osoby 262

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

9.4.3 Ochrana osobných údajov v infozákone 267
9.4.4 Závery 273
9.5 AUTOMATIZOVANÉ ROZHODOVACIE SYSTÉMY 274
9.5.1 Osobitná úprava v GDPR 274
9.5.2 Výlučne automatizované spracovanie 277
9.5.2.1 Právo alebo zákaz? 278
9.5.2.2 Výnimky 279
9.5.2.3 Nevyhnutnosť uzavretia alebo plnenia zmluvy 279
9.5.2.4 Súhlas 280
9.5.2.5 Povolenie právom 280
9.5.2.6 Osobitné kategórie osobných údajov 283
9.5.2.7 Vhodné opatrenia 283
9.5.2.8 Kde sú zástupcovia zamestnancov? 284
9.5.2.9 Právo na ľudský zásah 284
9.5.2.10 Dôsledky nedodržania Článku 22 285
10 PRACOVNOPRÁVNE INŠTITÚTY SÚVISIACE S MONITOROVANÍM ZAMESTNANCOV 286
10.1 DÔSTOJNOSŤ ZAMESTNANCA V PRACOVNOPRÁVNOM VZŤAHU 286
10.2 DIGITÁLNE HROZBY NA PRACOVISKU A OCHRANA SÚKROMIA ZAMESTNANCA 287
10.2.1 Šikana a kyberšikana na pracovisku 288
10.2.2 Mobbing a bossing na pracovisku 290
10.2.3 Obťažovanie a sexuálne obťažovanie 291
10.2.4 Digitálny pokyn na diskrimináciu 291
10.2.5 Monitorovacie programy ako prevencia pred digitálnym násilím 292
10.3 Duševné zdravie zamestnanca a technostres 293
11 ZÁVERY - BUDÚCNOSŤ A PERSPEKTÍVA OCHRANY OSOBNÝCH ÚDAJOV A SÚKROMIA ZAMESTNANCA 295
11.1 ZOVŠEOBECŇUJÚCE ZÁVERY 295
11.2 ZÁVERY K ROZHODOVACEJ PRAXI SÚDNYCH AUTORÍT 298
11.3 ZÁVERY K OCHRANE SÚKROMIA V INTENCIÁCH GDPR A ZÁKONA O OCHRANE OSOBNÝCH ÚDAJOV 305
11.4 K OTÁZKE ROZŠÍRENIA OCHRANY OSOBNÝCH ÚDAJOV NA PRÁVNICKÉ OSOBY 306
ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV 308

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ÚVOD

Otázky vplyvu judikatúry na formovanie právnej vedy ako aj v opozite otázky vplyvu právnej vedy na judikatúru majú pre vnímanie aktuálnych problémov teórie pracovného práva veľmi veľký význam. Vzhľadom na skutočnosť, že pracovnoprávna legislatíva je z hľadiska početnosti prijímaných zmien jednou z najčastejšie meniacich sa súčastí právneho poriadku, je viac než vysoko aktuálna a dôležitá ich aplikácia a interpretácia slovenskými súdmi. Z hľadiska témy tohto analýzy sa budeme zaoberať najmä analýzou vybraných rozhodnutí Ústavného súdu Slovenskej republiky (ďalej len „Ústavný súd“) vo vzájomnej korelácií s právnou úpravou vybraných sociálnych práv. Z teoretického hľadiska poskytneme pohľad do definičných znakov a charakteristiky vybraných sociálnych práv a zhodnotíme vplyv judikatúry na ich zotrvávanie, resp. zakotvenie v právnom poriadku. Pri spracovaní témy bude nevyhnutné použiť súhrn vedeckých metód ako je napríklad metóda analýzy a syntézy existujúcej právnej úpravy, metóda logického i gramatického výkladu právnych noriem, i textov konkrétnych rozhodnutí súdov.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

1 SOCIÁLNE PRÁVA – TEORETICKÉ VYMEDZENIE

Pri analýze skúmanej problematiky bude predmetom skúmania súbor sociálnych práv a ich zakotvenie v jednotlivých právnych predpisoch a zároveň zvýraznenie ich významu z hľadiska požiadaviek praxe.

1.1 PRÁVO NA OCHRANU OSOBNÝCH ÚDAJOV A SÚKROMIA V SYSTEMATIKE ĽUDSKÝCH PRÁV

Sociálne práva tvoria ťažiskovú časť právnej úpravy zákona č. 311/2011 Z.z., Zákonník práce v znení neskorších predpisov (ďalej len „Zákonník práce“), avšak ich podstatu nachádzame v zákone č. 460/1922 Zb., Ústava Slovenskej republiky v znení ústavných zákonov (ďalej len “Ústava SR“). Sociálne práva patria medzi základné práva, ktoré sú na rovnakej úrovni ako ústavné práva a slobody. Sú formulované všeobecne a v mnohých prípadoch majú programový charakter. Deklarujú jednu zo základných úloh štátu, t.j. starostlivosť o vytvorenie sociálnych predpokladov uplatnenia individuálnej slobody. Samotná identita pracovného práva už od samotného jeho vzniku je spätá so sociálnymi právami ako ľudskými právami druhej generácie. Základom sociálnych práv je rovnosť, sociálna bezpečnosť a sociálna spravodlivosť, na rozdiel od základných ľudských práv, ústavných slobôd občanov, základnou substanciou, ktorých je sloboda. Pre pracovné právo je charakteristické, že sa v jeho rámci uskutočňujú nielen typické sociálne ústavne práva občanov, ale aj typické liberálne slobody, ktoré aj napriek zaužívanému členeniu základných práv majú v rámci pracovnoprávnych vzťahov svoju špecifickú sociálnu substanciu. Vychádzajúc z uvedeného je evidentné, že zabezpečovanie sociálnych práv štátom je stále sa meniacim procesom. Ich realizácia je do značnej miery ovplyvňovaná aktuálnym vývojom hospodárstva v krajine. Sociálne a hospodárske práva potrebujú v prevažnej miere na svoju realizáciu konkretizáciu v bežných zákonoch, ktoré upravujú podmienky, či podrobnosti ich výkonu. Sociálne práva nie sú priamo vyvoditeľné z ich ústavného zakotvenia. Naopak ustanovenia Ústavy musia byť v danom prípade doplnené podrobnejšími ustanoveniami zákona. Týchto práv sa teda nemožno domáhať ex constitutione ale výlučne ex lege. Teória štátneho práva rozlišuje pojmy ústavné práva, ktoré vznikajú priamo z ústavy, a ústavné práva, ktoré vznikajú zo zákonov vykonávajúcich ústavu. V danom prípade hovoríme o tzv. blanketných normách, ktoré majú svoje odvodenie priamo z Ústavy a jej článku 51:

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

„Domáhať sa práv uvedených v čl. 35, 36, 37 ods. 4, čl. 38 až 42 a čl. 44 až 46 tejto ústavy sa možno len v medziach zákonov, ktoré tieto ustanovenia vykonávajú.“ Objavujú sa aj názory, ktoré označujú tieto práva ako neústavné, pretože nachádzajú svoju priamu realizáciu až na základe zákonnej úpravy a to napriek faktu, že zakotvené v ústave. Pojmový a terminologický problém je nielen vo vnútroštátnej právnej úprave, ale aj v medzinárodnej úprave. Medzinárodná úprava, ktorá sa dotýka práv a slobôd obsahuje ľudské práva uvádzané pod názvom a obsahom Medzinárodného paktu o občianskych a politických právach, ako aj Medzinárodného paktu o hospodárskych, sociálnych a kultúrnych právach. V týchto dokumentoch ako aj vo Všeobecnej deklarácii ľudských práv sú práva a slobody zakotvené v tom najširšom vyjadrení. Európsky dohovor o ochrane ľudských práv a základných slobôd vo svojom obsahu zakotvuje aj práva slobody, ktoré sú v Ústave Slovenskej republiky uvedené v iných oddieloch. Podobne v poslednom období medzinárodné orgány ako napríklad Európsky súd pre ľudské práva začínajú používať pojem ľudské práva na práva hospodárske, sociálne a kultúrne. Základné ľudské práva je možné charakterizovať ako skupinu práv, ktoré sú najviac spojené s osobnou integritou jednotlivca, človeka s jeho podstatou, živou osobou a osobnosťou. V odbornej právnickej literatúre sa z tejto vyčleňuje skupina práv, ktoré sa dotýkajú výhradne osobnej integrity človeka, a pomenúvajú sa ako tzv. „osobnostné práva“. Celkove však pojmové a terminologické formulácie v Ústave Slovenskej republiky umožňujú, že ústavná úprava ľudských práv a slobôd je v súlade s medzinárodnou právnou úpravou a jej princípmi. Ústavné zakotvenie práva na prácu je koncipované v porovnaní s úpravou v Zákonníku práce vzhľadom na jeho osobný rozsah oveľa užšie. Ústava SR totiž zakotvuje právo na prácu pre občanov („čl. 35 ods.3) Občania majú právo na prácu. Štát v primeranom rozsahu hmotne zabezpečuje občanov, ktorí nie z vlastnej viny nemôžu toto právo vykonávať. Podmienky ustanoví zákon.) .

1.2 AUTONÓMIA A SÚKROMIE JEDNOTLIVCA

Autonómia jednotlivca v pracovnom práve je základným predpokladom vzniku pracovnoprávnych vzťahov. Z teórie vyplýva, že pracovné právo ako samostatné právne odvetvie je súborom právnych noriem, ktoré upravujú vzťahy medzi ľuďmi pri uskutočňovaní ľudskej práce. Z hľadiska teoretického vymedzenia tieto vzťahy nazývame v širšom slova

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zmysle pracovnoprávnymi vzťahmi. V užšom zmysle slova sú pracovnoprávne vzťahy všetky právne vzťahy týkajúce sa výkonu práce bez ohľadu na to, na základe akých právnych noriem vznikajú, menia sa a zanikajú. Z hľadiska subjektívnej stránky rozlišujeme pracovnoprávne vzťahy na individuálne a kolektívne. Individuálne pracovnoprávne vzťahy sú vzťahy medzi individuálnymi subjektmi, v našom prípade medzi zamestnancom na jednej strane a zamestnávateľom na strane druhej. V prípade ak v pracovnoprávnom vzťahu vystupuje kolektívny subjekt, hovoríme o tzv. kolektívnych pracovnoprávnych vzťahoch. Subjektmi kolektívnych pracovnoprávnych vzťahov sú na jednej strane zamestnávateľ, alebo tzv. organizácie zamestnávateľov, a na strane druhej sú samotní zamestnanci, alebo zástupcovia zamestnancov. predstavujú vzťahy, kde aspoň na jednej strane vystupuje kolektívny subjekt. Kolektívne pracovnoprávne vzťahy sú doplnením individuálnych pracovnoprávnych vzťahov a v istom zmysle ich aj chránia. Popri individuálnych a kolektívnych pracovnoprávnych vzťahoch sa v praxi stretávame aj s tzv. ďalšími pracovnoprávnymi vzťahmi, ktoré majú svoje zákonné zakotvenie v iných právnych predpisoch ako je zákon č. 311/2001 Z. z., Zákonník práce v znení neskorších predpisov, (ďalej len „Zákonník práce“), ktorý sa ne vzťahuje len delegovane, resp. subsidiárne. Do tejto skupiny pracovnoprávnych vzťahov zaraďujeme pracovné vzťahy, ktoré sa realizujú v inom právnom vzťahu ako je pracovný pomer (napr.: štátnozamestnanecký pomer, služobný pomer, ako aj ostatné pracovné vzťahy, ktoré vznikajú pri výkone verejnej funkcie, resp. vzťahy sudcov k štátnej moci, vzájomné vzťahy členov družstiev - pokiaľ ich súčasťou je výkon práce).

1.2.1 Subjekty individuálnych pracovnoprávnych vzťahov

Pojem subjekt pracovnoprávnych vzťahov je potrebné odlišovať od pojmu subjekt pracovného práva. Rozdiel spočíva najmä v tom, že subjekt pracovnoprávneho vzťahu, alebo obdobného pracovného vzťahu (na rozdiel od subjektu pracovného práva) zrealizoval konkrétnu subjektívnu pracovnoprávnu skutočnosť, ktorá je prejavom vôle, t.j. právnym úkonom, ktorý musí vykazovať zákonom stanovené kritériá. Ako už bolo v úvode načrtnuté medzi subjekty individuálnych pracovnoprávnych vzťahov zaraďujeme zamestnávateľa a zamestnanca.

1.2.1.1 Zamestnávateľ

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Pojem zamestnávateľ je v § 7 ods. 1 Zákonníka práce definovaný ako právnická osoba alebo fyzická osoba, ktorá zamestnáva aspoň jednu fyzickú osobu v pracovnoprávnom vzťahu, a ak to ustanovuje osobitný predpis, aj v obdobných pracovných vzťahoch. V zmysle zákonnej úpravy vystupuje zamestnávateľ v pracovnoprávnych vzťahoch vo svojom mene a za svoje konanie nesie zodpovednosť. Ako vyplýva zo zákonnej definície zamestnávateľom môže byť fyzická osoba, právnická osoba, a taktiež aj organizačná jednotka zamestnávateľa. Ak je zamestnávateľom fyzická osoba musí spĺňať zákon stanovené podmienky, teda musí mať tzv. pracovnoprávnu subjektivitu. Ako už bolo spomenuté pri pracovnoprávnych vzťahoch pracovnoprávna subjektivita pozostáva zo a) spôsobilosti mať práva a povinnosti - pasívna zložka, b) spôsobilosti na právne úkony - aktívna zložka, c) deliktuálna spôsobilosť, d) procesná spôsobilosť. V tomto prípade spôsobilosť fyzickej osoby mať práva a povinnosti v pracovnoprávnych vzťahoch ako zamestnávateľ vzniká narodením, pričom ju má aj počaté dieťa, ak sa narodí živé. Na druhej strane spôsobilosť fyzickej osoby vlastnými právnymi úkonmi nadobúdať práva a brať na seba povinnosti v pracovnoprávnych vzťahoch ako zamestnávateľ vzniká plnoletosťou, pričom do jej dosiahnutia za ňu koná zákonný zástupca. V zmysle § 8 ods. 2 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov sa plnoletosť nadobúda dovŕšením osemnásteho roku, pričom pred dosiahnutím tohto veku sa plnoletosť nadobúda len uzavretím manželstva. Takto nadobudnutá plnoletosť sa nestráca ani zánikom manželstva ani vyhlásením manželstva za neplatné. V tomto prípade koná fyzická osoba v pracovnoprávnych vzťahoch osobne. Keďže Zákonník práce neupravuje zánik spôsobilosti zamestnávateľa ako fyzickej osoby, subsidiárne použijeme Občiansky zákonník, v zmysle ktorého táto spôsobilosť zaniká smrťou a ak smrť nemožno preukázať predpísaným spôsobom, súd fyzickú osobu vyhlási za mŕtvu, ak zistí jej smrť inak. Za mŕtveho súd vyhlási aj nezvestnú fyzickú osobu, ak so zreteľom na všetky okolnosti možno usúdiť, že už nežije (§ 7 ods. 2). Zákonník práce nedefinuje ani pracovnoprávnu subjektivitu zamestnávateľa ako právnickej osoby. V danom prípade opäť vychádzajúc z úpravy v Občianskom zákonníku môžeme konštatovať, že podľa § 18 a nasl. spôsobilosť mať práva a povinnosti majú aj právnické osoby, ktorými sú a) združenia fyzických alebo právnických osôb, b) účelové združenia majetku, c) jednotky územnej samosprávy a d) iné subjekty, o ktorých to ustanovuje zákon. Pri právnických osobách rozlišujeme dva okamihy ich vzniku, pričom sa rozlišuje medzi

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zriadením a vznikom. Na jednej strane na zriadenie právnickej osoby je potrebná písomná zmluva alebo zakladacia listina, ale na strane druhej vzniká až dňom, ku ktorému je zapísaná do obchodného alebo do iného zákonom určeného registra, pokiaľ osobitný zákon neustanovuje jej vznik inak. Spôsobilosť právnickej osoby nadobúdať práva a povinnosti môže byť obmedzená len zákonom a vzniká dňom účinnosti zápisu do spomínaného registra. Vychádzajúc zo spomínanej občianskoprávnej úpravy môžeme definovať aj okamih zániku právnickej osoby, pričom sa opäť rozlišuje medzi zrušením a zánikom. Právnická osoba sa zrušuje dohodou, uplynutím doby alebo splnením účelu, na ktorý bola zriadená a pokiaľ je zapísaná v obchodnom registri alebo v inom zákonom určenom registri zaniká dňom výmazu z tohto registra, pokiaľ osobitné zákony neustanovujú inak. V tomto prípade pracovnoprávna subjektivita právnickej osoby zaniká týmto dňom. V pracovnoprávnych vzťahoch robí právne úkony za zamestnávateľa - právnickú osobu, štatutárny orgán alebo člen štatutárneho orgánu, pričom môžu namiesto nich robiť právne úkony aj nimi poverení zamestnanci. Iní zamestnanci zamestnávateľa, najmä vedúci jeho organizačných útvarov, sú oprávnení ako orgány zamestnávateľa robiť v mene zamestnávateľa právne úkony vyplývajúce z ich funkcií určených organizačnými predpismi, a taktiež môže zamestnávateľ písomne poveriť ďalších svojich zamestnancov, aby robili určité právne úkony v pracovnoprávnych vzťahoch v jeho mene, pričom v danom poverení musí byť uvedený rozsah ich oprávnenia.

1.2.1.2 Zamestnanec

Pojem zamestnanec definuje Zákonník práce v § 11 ods. 1 - zamestnancom je fyzická osoba, ktorá v pracovnoprávnych vzťahoch, a ak to ustanovuje osobitný predpis, aj v obdobných pracovných vzťahoch vykonáva pre zamestnávateľa závislú prácu. Za zamestnanca je potrebné podľa pracovnoprávnej teórie považovať aj fyzickú osobu, ktorá je v neplatnom pracovnoprávnom vzťahu, t. j. vo faktickom pracovnom pomere. Na rozdiel od fyzickej osoby zamestnávateľa vzniká spôsobilosť fyzickej osoby mať v pracovnoprávnych vzťahoch práva a povinnosti ako zamestnanec ako aj spôsobilosť vlastnými právnymi úkonmi nadobúdať tieto práva a brať na seba tieto povinnosti, dňom, keď fyzická osoba dovŕši 15 rokov veku (možnosť uzatvoriť dohodu o hmotnej zodpovednosti má až najskôr v deň, keď dovŕši 18 rokov veku). Podmienkou v danom prípade, ale je, že zamestnávateľ nesmie s touto osobou dohodnúť v

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

pracovnej zmluve, alebo dohode, ako deň nástupu do práce deň, ktorý by predchádzal dňu, keď fyzická osoba skončí povinnú školskú dochádzku. Povinná školská dochádzka je podľa zákona č. 245/2008 Z.z. o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov stanovená na dĺžku desať rokov, pričom sa začína začiatkom školského roka, v roku keď už dieťa dovŕšilo šiesty rok veku. Ak dieťa po dovŕšení šiesteho roku veku nie je spôsobilé začať navštevovať základnú školu, kompetentný orgán štátnej správy v školstve rozhodne o jeho zaradení do nultého ročníka základnej školy alebo o odklade začiatku povinnej školskej dochádzky o jeden školský rok. Povinná školská dochádzka trvá najdlhšie do konca školského roku, v ktorom žiak dovŕšil šestnásty rok veku, ak zákon neustanovuje inak. Vzhľadom na uvedené to vyzerá tak, že mladistvý môže začať vykonávať závislú prácu po skončení prvého ročníka na strednej škole. Teda pokiaľ hovoríme o zamestnancovi mladšom ako 18 rokov, nazývame ho v zmysle § 40 ods. 3 Zákonníka práce mladistvý zamestnanec. Mladistvý zamestnanec požíva v pracovnoprávnych vzťahoch osobitnú ochranu. Zákonník práce definuje pojem detskej práce, tým, že konštatuje, že práca fyzickej osoby vo veku do 15 rokov alebo práca fyzickej osoby staršej ako 15 rokov do skončenia povinnej školskej dochádzky je zakázaná, pričom tieto osoby môžu vykonávať iba ľahké práce, ktoré svojím charakterom a rozsahom neohrozujú ich zdravie, bezpečnosť, ich ďalší vývoj alebo školskú dochádzku. Pod pojmom ľahké práce rozumieme práce pri účinkovaní alebo spoluúčinkovaní na kultúrnych predstaveniach a umeleckých predstaveniach, športových podujatiach, alebo reklamných činnostiach. Smrťou fyzickej osoby zamestnanca dochádza k zániku pracovného pomeru, ale nie k zániku jeho práv a povinností. Zákonník práce upravuje v § 35 otázku peňažných nárokov po jeho smrti, pričom konštatuje, že peňažné nároky zamestnanca jeho smrťou nezanikajú a do štvornásobku jeho priemerného mesačného zárobku prechádzajú postupne priamo na jeho manžela, deti a rodičov, ak s ním žili v čase smrti v domácnosti a predmetom dedičstva sa stávajú až, ak týchto osôb niet. Na strane druhej konštatuje, že peňažné nároky zamestnávateľa voči zomrelému zamestnancovi zanikajú jeho smrťou s výnimkou nárokov, o ktorých sa právoplatne rozhodlo alebo ktoré zamestnanec pred svojou smrťou písomne uznal čo do dôvodu aj sumy, a nárokov na náhradu škody spôsobenej úmyselne alebo stratou predmetov zverených zamestnancovi na písomné potvrdenie.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

1.2.2 Autonómia jednotlivca a zásada zmluvnosti

Autonómia jednotlivca v individuálnych pracovnoprávnych vzťahoch sa prejavuje predovšetkým v tzv. zmluvnej slobode, ktorá sa prejavuje najmä v možnosti uzavrieť pracovný pomer pracovnou zmluvou. Práve pri vzniku pracovného pomeru majú byť zásade zmluvnej slobody, resp. zmluvnosti ponechané veľmi široké hranice. V praktickom živote existujú určité faktické okolnosti, ktoré majú vplyv na slobodu uzavrieť pracovnú zmluvu. Nedotýkajú sa však podstaty zmluvnej slobody, ale iba skutkovo vymedzujú priestor, v ktorom je vykonávaná právom garantovaná sloboda uzavrieť zmluvu. V súčasnej dobe je zmluvná sloboda obmedzovaná nielen pri uzatváraní pracovnej zmluvy, ale predovšetkým v priebehu pracovného pomeru, a to výrazne v prospech zamestnanca. Táto zásada je odzrkadlením nerovného postavenia subjektov pracovnoprávneho vzťahu. Napriek názoru niektorých autorov , že nie je možné od zvýšenej ochrany zamestnancov odvodzovať, že ochranná funkcia pracovného práva by sa mala týkať iba zamestnancov, ba naopak chrániť všetky subjekty pracovnoprávnych vzťahov, je nevyhnutné poznamenať, že podriadené a slabšie postavenie zamestnancov ako subjektu pracovnoprávnych vzťahov si odôvodnene vyžaduje zvýšenú ochranu oproti silnejšiemu postaveniu zamestnávateľov.

Právnym základom zmluvnej slobody, ktorá je v teórii definovaná ako zásada zmluvnosti je čl. 2 Zákonníka práce . Táto zásada sa prejavuje nielen pri založení, ale aj pri zmene a skončení pracovnoprávnych vzťahov. Zásadným predpokladom pre túto zásadu je uplatňovanie osobnej slobody (vychádza a je založená na súkromnej autonómii osoby) zaručenej v čl. 17 Ústavy SR vo vzájomnej korelácii so spôsobilosťou na právne úkony. Podľa prof. Barancovej sa rešpektovanie osobnej slobody zamestnanca prejavuje najmä pri uzatváraní pracovnej zmluvy. Princíp zmluvnej autonómie znamená takú právnu kvalitu zmluvnej voľnosti, v rámci ktorej subjekt sám slobodne rozhoduje, či bude kontrahovať, s kým a akým obsahom naplní svoju kontraktáciu s iným. Základný obsahový rámec zmluvnej voľnosti v individuálnom pracovnom práve spočíva najmä v slobode výberu zmluvného partnera, slobode uzavretia zmluvy, slobode určenia obsahu zmluvy, slobode skončenia zmluvy a slobode výberu zmluvnej formy. Takto vymedzené slobody sa v pracovnoprávnych vzťahoch sa však neuplatňujú neobmedzene. Samotný základný pracovnoprávny predpis zakotvuje niekoľko obmedzení

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

týchto slobôd. V tomto smere jedine sloboda výberu zmluvného partnera je determinovaná zákonnými podmienkami len do tej miery, že pri výbere zmluvného partnera musí byť naplnená podmienka právnej, resp. pracovnoprávnej subjektivity, teda spôsobilosti byť subjektom pracovnoprávneho vzťahu. Tieto podmienky sú bližšie definované v predchádzajúcej kapitole. Sloboda výberu zmluvného partnera, ako aj sloboda uzavretia zmluvy má svoj právny základ už v spomínanom v čl. 2 Zákonníka práce. Ďalšie uvedené slobody, najmä z hľadiska ich uplatňovania podliehajú istým obmedzeniam, ktoré nachádzame v príslušných ustanoveniach Zákonníka práce i osobitných právnych predpisov. Sloboda určenia obsahu zmluvy je ovplyvnená z hľadiska druhu zmluvy kogentnými ustanoveniami právnych predpisov, pričom príkladmo sloboda určenia obsahu pracovnej zmluvy ako predpokladu založenia pracovného pomeru je striktne viazaná na podstatné náležitosti ako sú miesto výkonu práce, deň nástupu do práce, druh práce, či mzdové podmienky. Obdobne Zákonník práce určuje obsahové náležitosti aj pri iných zmluvných typoch. To isté platí aj pri slobode určenia zmluvnej formy, pričom vo väčšine prípadov je ustanovená povinnosť písomnej formy zmluvy, pod sankciou neplatnosti (s výnimkou pracovnej zmluvy) v korelácii s § 17 Zákonníka práce o neplatnosti právnych úkonov. Uplatňovanie slobody skončenia zmluvy je potrebné analyzovať z hľadiska toho ktorého subjektu zmluvného vzťahu. To platí najmä pri slobode skončenia pracovného pomeru ako základného zmluvného vzťahu v pracovnom práve, pretože Zákonník práce rozlišuje medi autonómiou zamestnanca a autonómiou zamestnávateľa. V tomto prípade sa zjavne prejavuje ochranná funkcia pracovného práva tým, že ustanovuje presne dôvody na skončenie zmluvného vzťahu (pracovného pomeru) zo strany zamestnávateľa vymedzením tzv. výpovedných dôvodov. V prípade výpovede z pracovného pomeru zo strany zamestnanca ponecháva Zákonník práce úplnú autonómiu zamestnancovi tým, že neurčuje dôvody, na základe ktorých môže podať výpoveď. Naopak obmedzenia slobody skončenia zmluvy sú vymedzené pri okamžitom skončení pracovného pomeru a to konkrétnymi dôvodmi, ktoré sú definované tak pre zamestnávateľa, ako zamestnanca.

Autonómia jednotlivca – tak zamestnanca ako i zamestnávateľa v individuálnych pracovnoprávnych vzťahov je odvodená od jednej zo základných zásad pracovného práva – od zásady zmluvnosti. Tá sa vzhľadom na charakter týchto vzťahov uplatňuje pri vzniku, zmene,

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

či skončení zmluvného vzťahu v pracovnom práve. Jej realizácia je výrazne determinovaná obmedzeniami, ktoré sú ustanovené v Zákonníku práce (resp. osobitných právnych predpisoch). Autonómne uplatňovanie slobôd z nej vyplývajúcich podlieha pravidlám, ktoré vo väčšine prípadov ich nedodržania spájajú takto „nedokonalý" právny úkon so sankciou neplatnosti. Táto skutočnosť je však prejavom najmä ochrannej funkcie pracovného práva, ktorá vyúsťuje do systému uzavretých zmluvných typov pracovného práva.

1.3 PRAMENE PRÁVA UPRAVUJÚCE OCHRANU OSOBNÝCH ÚDAJOV A SÚKROMIA

1.3.1 Všeobecne k prameňom práva

Prameň práva je pojem, ktorý má viacero významov, v ktorých je konkrétne právo obsiahnuté. V teórii práva sa spravidla rozlišujú pramene práva vo formálnom zmysle a pramene práva v materiálnom zmysle. Materiálne pramene práva predstavujú ekonomické, sociálne, demografické, geografické, prírodné, politické, mravné a ekologické, technologické, politické a rôzne iné faktory, ktoré vplývajú na tvorbu práva. Z týchto faktorov tvorba práva taktiež vychádza. Formálne pramene práva sú zdrojom, v ktorom je samotné právo obsiahnuté, pramení z neho, možno ho v týchto formách identifikovať ako právo vydané štátom. Na základe týchto skutočností sa potom môžeme dožadovať splnenia, alebo uplatnenia. Jedným z dôležitých znakov práva je jeho forma. S prihliadnutím na konkrétny právny systém rozoznávame formu práva vo všeobecnom zmysle a v osobitnom zmysle slova. Vo všeobecnom zmysle predstavuje forma práva špecifický znak práva. Z toho dôvodu dochádza k odlíšeniu práva od iných spoločenských noriem (politiky, športu, morálky), a taktiež k existencií samotného práva. V osobitnom zmysle predstavuje forma práva špecifický znak práva určitého štátu. Z dôvodu existencie rôznorodosti národných právnych systémov a právnych kultúr poznáme aj rôznorodé formy práva. Všeobecne sa v typoch právnej kultúry pochádzajúcich z Európy rozoznávajú tieto hlavné druhy prameňov práva:

- normatívne právne akty (právne predpisy),
- právne obyčaje,
- súdne precedensy,

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- normatívne zmluvy,
- iné formy (pramene) práva.[1]

Právny poriadok Slovenskej republiky patrí do kontinentálneho typu právnej kultúry, pre ktorý je typické tzv. písané právo. Má svoju hierarchickú štruktúru, ktorá spočíva v tom, že na vrchole je Ústava a ústavné zákony, následne zákony, ktoré musia byť v súlade s Ústavou a ústavnými zákonmi, ďalej vykonávacie právne predpisy, ktoré musia byť v súlade s predchádzajúcimi prameňmi. Osobitnou kategóriou sú v zmysle čl. 7 ods. 5 Ústavy medzinárodné zmluvy o ľudských právach a základných slobodách, medzinárodné zmluvy, na ktorých vykonanie nie je potrebný zákon, a medzinárodné zmluvy, ktoré priamo zakladajú práva alebo povinnosti fyzických osôb alebo právnických osôb a ktoré boli ratifikované a vyhlásené spôsobom ustanoveným zákonom, ktoré majú prednosť pred zákonmi.

1.4 DRUHY PRAMEŇOV PRACOVNÉHO PRÁVA

Pracovné právo ako samostatné odvetvie právneho poriadku, ktoré je výnimočné svojou hybridnou povahou, tvorenou súkromnoprávnymi i verejnoprávnymi prvkami, je výnimočné aj vo výpočte a definícii jeho formálnych prameňov. Patria sem:

- Normatívne právne akty.
- Kolektívne zmluvy.
- Vnútropodnikové normatívne akty.
- Technické normy.
- Dobré mravy.
- Medzinárodne zmluvy.
- Právne záväzné akty Európskej únie.

1.4.1 Európske pramene

[1] K tomu pozri bližšie: PRUSÁK, J. Teória práva. 2. vyd. Bratislava: Vydavateľské oddelenie PF UK, 2001. ISBN 80-7160-146-2, 188 s.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Právo na rešpektovanie súkromného života zamestnanca je zakotvené v článku 8 Európskeho dohovoru ochrane ľudských práv a základných slobôd (ďalej len: *„Dohovor"*) a v Charte základných práv EÚ (ďalej len: *„Charta"*). Podľa čl. 8 Dohovoru má každý právo na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie. Právo na súkromný život patrí medzi základné ľudské práva prvej generácie. Podľa čl. 7 Charty má každá osoba právo na ochranu súkromného a rodinného života, právo na obydlie a komunikáciu, pričom predmetom ochrany práva na rešpektovanie komunikácie je práve korešpondencia, avšak právna ochrana nezahŕňa len písomnú korešpondenciu, ale akúkoľvek inú komunikáciu prostredníctvom telefonických rozhovorov, počas ktorých podlieha právnej ochrane aj tretia osoba, s ktorou fyzická osoba telefonuje.[2] Podľa čl. 12 Všeobecnej deklarácie ľudských práv nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromného života, rodiny, domova alebo korešpondencie, ani útokom na svoju česť a povesť. Každý má právo na zákonnú ochranu pred takýmto zásahom alebo útokom. Obdobne je ochrana súkromia nie len zamestnancov obsiahnutá v čl. 17 Medzinárodného dohovoru o občianskych a politických právach. V Slovenskej republike je ochrana súkromia zaručená v čl. 16 zákona č. 460/1992 Zb. Ústava Slovenskej republiky v znení neskorších predpisov, podľa ktorého nedotknuteľnosť osoby a jej súkromia je zaručená. Podľa čl.11 Zákonníka práce zamestnávateľ môže o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával. Ochrana súkromia je predmetom legislatívnej úpravy aj v § 11 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov, podľa ktorého má fyzická osoba právo na ohranu svojej osobnosti, najmä života a zdravia, občianskej cti a ľudskej dôstojnosti, ako aj súkromia, svojho mena a prejavov osobnej povahy.

V rámci ochrany súkromného života zamestnanca sú osobitne chránené osobné údaje zamestnanca. Ochrana osobných údajov je v práve EÚ predmetom osobitnej legislatívnej úpravy, ktorá je vyjadrená najmä v smerniciach. Jedná sa o Smernicu Európskeho parlamentu a Rady č. 95/46 ES zo dňa 24. októbra 1995 o ochrane jednotlivcov vzhľadom na spracovávanie

[2] Rozhodnutie ESĽP v právnej veci Klass z roku 1978.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

osobných údajov a o voľnom pohybe takých údajov (ďalej len: *„Smernica“*). Dňa 04. mája 2016 bolo v Úradnom vestníku Európskej únie zverejnené Nariadenie Európskeho Parlamentu a Rady 2016/679 z 27 apríla 2016 o ochrane fyzických osôb pri spracovaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len: *„Nariadenie“*). Týmto Nariadením sa zrušuje Smernica a toto Nariadenie nadobudne účinnosť dňa 25. mája 2018, pričom do uvedeného obdobia sa v Slovenskej republike bude naďalej aplikovať zákon č. 122/ 2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.[3]

1.4.2 Vnútroštátne pramene

Ochrana súkromia v pracovnoprávnych vzťahoch je v súčasnosti v pracovnoprávnej teórii veľmi diskutovanou témou. Tieto odborné diskusie sú vyvolávané najmä otázkami, ktoré vyvstávajú v praktickom živote pri realizácií práv a povinností vyplývajúcich z pracovnoprávnych vzťahov. Zamestnávatelia v snahe maximalizovať zisk a minimalizovať straty často krát neváhajú zasahovať do základných práv zamestnancov s odôvodnením potreby ochrany ich majetku a záujmov na ochrane pred neblahými konkurenčnými praktikami ich konkurentov na hospodárskom trhu. Právny rámec ochrany súkromia je daný v prvom rade v čl. 8 ods. 1 Európskeho dohovoru o ochrane ľudských práv[4] a následne nachádza svoje ústavné zakotvenie v čl. 19 ods. 2 zákona č. 460/1992 Zb., Ústava Slovenskej republiky ako vyplýva zo zmien a doplnení vykonaných ústavnými zákonmi (ďalej len „Ústava SR“).[5] Z hľadiska systematiky Ústavy SR patrí toto právo medzi Základné ľudské práv a slobody. Samotná Ústava SR v čl. 13 ustanovuje možnosť obmedzenia základných práv a slobôd a to tak, že *„medze základných práv a slobôd možno upraviť za podmienok ustanovených touto ústavou len zákonom“* a, že *„zákonné obmedzenia základných práv a slobôd musia platiť rovnako pre všetky prípady, ktoré spĺňajú ustanovené podmienky.“* Takto definované právo na ochranu súkromia platí teda aj na úrovni pracovnoprávnych vzťahov. Táto ochrana je definovaná ako ochrana súkromia zamestnanca, pričom je zákonne limitovaná právom zamestnávateľa a jeho oprávnenými záujmami súvisiacimi s pracovnoprávnymi vzťahmi.

[3] ŠVEC, M., VALENTOVÁ, T.: Ochrana osobných údajov v pracovnoprávnych vzťahoch. 1. vyd. Bratislava: WoltersKluwer, 2016, 19, ISBN: 978-80-8168-493-6.
[4] „Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie.“
[5] „Každý má právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života.“

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Oprávnené záujmy zamestnávateľa zasahovať do súkromia zamestnanca sa v zmysle platnej právnej úpravy vzťahujú nielen na pracoviska zamestnávateľa a spoločné priestory zamestnávateľa, ale súvisia aj s právom zamestnávateľa na kontrolu dodržiavania liečebného režimu zamestnancov. V zásade však platí, že zásahy zamestnávateľa do súkromia zamestnanca musia byť v súlade so zásadou legality, legitimity a proporcionality.[6] V prípade zamestnávateľa sa možno stretnúť s jeho právom na ochranu majetku, ktorý zveruje svojmu zamestnancovi. Zamestnávateľ má právo kontrolovať, akým spôsobom a v akom rozsahu zamestnanec používa zverené prostriedky. V praxi sa však objavujú prípady, že sa v rámci monitorovania činnosti zamestnanca dostáva právo zamestnávateľa na ochranu jeho majetku, ako aj jeho právo na kontrolu vykonávania práce do kolízie s právom na ochranu súkromia zamestnanca.

1.4.3 Právna úprava ochrany súkromia v pracovnoprávnych predpisoch

Zákonný rámec ochrany súkromia zamestnancov a možných zásahov do ich súkromia zo strany zamestnávateľa je stanovený v základnom pracovnoprávnom predpise, v zákone č. 311/2001 Z.z., Zákonník práce v znení neskorších predpisov (ďalej len „Zákonník práce“), ktorý nadobudol účinnosť dňa 1. apríla 2002, okrem § 5 ods. 2 až 5 a § 241 až 245, ktoré nadobudli účinnosť vstupom Slovenskej republiky do Európskej únie. Vychádzajúc z pôvodnej právnej úpravy bol pre túto problematiku podstatný článok 11 Základných zásad Zákonníka práce, podľa ktorého *„Zamestnávateľ môže o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával. Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho sleduje bez toho, aby bol na to upozornený, alebo kontroluje listové*

[6] Podrobnejšie pozri Musil, J.-Švestka, J.-Holländer,P.: Bezpečnostní výzvy a omezení základních práv v postmoderní realitě. Právní aspekty situace po 11. září 2001, Brno: Masarykova univerzita v Brně, Mezinárodní politologický ústav, 2002, 94 – 106 s. Čentéš, J.–Lazareva, N.: Legalita, legitimita a proporcionalita odpočúvania a zaznamenávania telekomunikačnej prevádzky. Zborník príspevkov z celoštátnej konferencie s medzinárodnou účasťou „Aktuálne otázky trestného zákonodarstva“ – pocta akademikovi, Dr. H. c. prof. JUDr. Milanovi Čičovi, DrSc. k 80. narodeninám, konanej dňa 19. januára 2012, Bratislava: Fakulta práva Paneurópskej vysokej školy, 183 – 198 s.
.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zásielky adresované zamestnancovi ako súkromnej osobe. Ak je u zamestnávateľa zavedený kontrolný mechanizmus, je zamestnávateľ povinný informovať zamestnanca o rozsahu kontroly a spôsoboch jej uskutočňovania." Pre vymožiteľnosť a aplikovateľnosť práva na ochranu súkromia zo strany zamestnancov však táto právna úprava nebola postačujúca. Z hľadiska systematiky sa nenachádzala v normatívnej časti Zákonníka práce, ale jej právny rámec bol iba deklaratórnym vyjadrením jej podstaty. V tejto súvisloti je nevyhnutné uviesť, že novelizácia Zákonníka práce zákonom č. 361/2012 Z. z., ktorým sa mení a dopĺňa zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony (ďalej len „novela Zákonníka práce"), ktorá nadobudla účinnosť 1. januára 2013, vypustila druhú a tretiu vetu v článku 11 Základných zásad Zákonníka práce a obsah tohto článku ustanovila v normatívnej časti Zákonníka práce v § 13 ods. 4.

Podľa § 13 ods. 4 novely Zákonníka práce: „ Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje a vykonáva záznam telefonických hovorov uskutočnených technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronickú poštu odoslanú z pracovnej elektronickej adresy a doručenú na túto adresu bez toho, aby ho na to vopred upozornil. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania."

Porovnaním článku 11 Základných zásad Zákonníka práce (druhá a tretia veta) a § 13 ods. 4 novely Zákonníka práce možno konštatovať, že zo znenia článku 11 Základných zásad Zákonníka práce novela Zákonníka práce vypúšťa kontrolu listových zásielok adresovaných zamestnancovi ako súkromnej osobe. Zároveň novela Zákonníka práce upresňuje niektoré spôsoby narušenia súkromia zamestnanca a kontrolný mechanizmus.[7] Novela Zákonníka

[7] Hamuľák, J.: Zmeny v právnej úprave Zákonníka práce – analýza a úvaha o platných a pripravovaných zmenách. Zborník príspevkov z medzinárodnej konferencie doktorandov a mladých vedeckých pracovníkov organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou. ,,Míľniky práva v stredoeurópskom priestore" Bratislava: PrafUK, 2011, 724 s.

.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

práce tiež ustanovuje právo zamestnanca, ktorý sa domnieva, že jeho súkromie na pracovisku alebo v spoločných priestoroch bolo narušené nedodržaním § 13 ods. 4, obrátiť sa na súd a domáhať sa právnej ochrany. V ďalšom texte venujeme pozornosť ustanoveniu § 13 ods. 4 novely Zákonníka práce, ktoré legalizuje nielen možnosť narušenia súkromia zamestnanca zamestnávateľom na pracovisku a spoločných priestoroch zamestnávateľa, ale aj podmienky a spôsoby zásahov do súkromia zamestnanca. V tomto ustanovení je ochrana súkromia vymedzená negatívne *„zamestnávateľ nesmie.“* V tejto súvislosti vzniká otázka, v ktorých prípadoch a za akých podmienok zamestnávateľ smie (je oprávnený) narušiť súkromie zamestnanca na pracovisku. Zamestnávateľ je oprávnený disponovať týmto oprávnením vtedy, ak:

- má na to vážne dôvody,
- vážny dôvod spočíva v osobitnej povahe činnosti zamestnávateľa,
- ide o narušenie súkromia na pracovisku alebo v spoločných priestoroch zamestnávateľa,
- spôsob narušenia súkromia zamestnanca spočíva v jeho monitorovaní, vyhotovení záznamu telefonických hovorov alebo kontrole elektronickej pošty, a to po predchádzajúcom upozornení zamestnanca.

Takáto úprava sa podľa odbornej literatúry javí ako vágna a nedostatočná. Polemika vzniká nad vymedzením uvedených pojmov, ktoré sú zákonnými predpokladmi akéhokoľvek monitoringu zamestnanca. Odhliadnuc od neurčitosti uvedených pojmov, zúženie monitoringu zamestnanca len na osobitné prípady je považované za príliš prísne a nezodpovedá rozumnému usporiadaniu a rovnováhe oprávnených záujmov zamestnávateľa a zamestnanca. Dôvod spočívajúci v *„osobitnej povahe činnosti zamestnávateľa“* je fakticky len jednou z podmienok, ktorá musí byť pre možnosť zásahu do súkromia zamestnanca naplnená. Druhou a nemenej významnou podmienkou je, že narušením súkromia zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa možno dosiahnuť sledovaný účel (napr. ochrana majetku zamestnávateľa). Zákon limituje možnosť narušenia súkromia zamestnanca, a to **pracoviskom a spoločnými priestormi**

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zamestnávateľa. Zamestnanec musí byť o možnosti a rozsahu kontroly vopred upozornený zamestnávateľom, pričom zákon neustanovuje spôsob tohto upozornenia. Zamestnávateľ túto okolnosť môže upraviť v jeho internom predpise, prípade v pracovnej zmluve. Novela Zákonníka práce ustanovuje niektoré spôsoby zásahu do súkromia zamestnanca. Na druhej strane možno konštatovať nedostatok právnej úpravy, ktorá neobsahuje striktné kritériá na použitie monitorovania, vykonávanie záznamu telefonických hovorov a kontrolu elektronickej pošty. Treba si uvedomiť, že záujmy zamestnávateľa ani pri existencii *„vážneho dôvodu“* nemôžu v žiadnom prípade byť nadradené právu zamestnanca na súkromie.

Novela Zákonníka práce v otázke zásahov do súkromia zamestnancov upravila aj účasť zástupcov zamestnancov, pričom Zákonník práce v § 11a ustanovuje účasť týchto zástupcov nasledovne – príslušný odborový orgán, zamestnanecká rada alebo zamestnanecký dôverník, zástupca zamestnancov pre bezpečnosť a ochranu zdravia pri práci podľa osobitného predpisu, ako aj osobitný orgán družstva volený členskou schôdzou, v prípade ak v družstve je súčasťou členstva aj pracovnoprávny vzťah člena k družstvu. V danom prípade je zamestnávateľ oprávnený kontrolovať zamestnancov po tom, ako prerokuje so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informuje zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania. Zástupcovia zamestnancov zohrávajú spravidla v otázkach zásahu do súkromia, resp. osobnej sféry zamestnancov zo strany zamestnávateľa významnú rolu. Ich prítomnosť vyvažuje existujúci faktický nepomer medzi subjektmi pracovného pomeru. Z uvedeného možno vyvodiť, že zamestnávateľ môže primeraným spôsobom kontrolovať svojich zamestnancov, ako nakladajú s hodnotami zverenými na výkon práce s tým, že kontrolou nesmie dochádzať k zásahom do osobnosti jednotlivca (§ 11 zákon č. 40/1964 Zb., Občiansky zákonník v znení neskorších predpisov), ibaže je daný vážny dôvod spočívajúci v osobitnej povahe činnosti zamestnávateľa. V takomto prípade je zamestnávateľ oprávnený zasiahnuť do súkromia zamestnanca. V prípade, ak pri kontrole zamestnávateľ zistí, že zamestnanec nevyužíva pracovný čas na prácu a riadne nehospodári s prostriedkami, ktoré mu boli zverené na výkon práce, je oprávnený postihnúť zamestnanca v zmysle pracovnoprávnych predpisov.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

K povinnostiam, ktoré sú zamestnanci povinní dodržiavať a ktoré legalizujú oprávnený záujem zamestnávateľa na isté zásahy do súkromia zamestnancov (súvisiace najmä s riadnym a osobným výkonom práce, ochranou majetku zamestnávateľa a riadneho nakladania a používania zverených prostriedkov zamestnávateľa), patria aj ďalšie povinnosti, ktoré ustanovuje Zákonník práce v § 81. V danom prípade je pre otázku ochrany súkromia podstatná najmä povinnosť v období, v ktorom má zamestnanec podľa osobitného predpisu nárok na náhradu príjmu pri dočasnej pracovnej neschopnosti, dodržiavať liečebný režim určený ošetrujúcim lekárom. Týmto osobitným predpisom je zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov, ktorý v § 9 ods. 4 dáva právo zamestnávateľovi vykonať kontrolu, či sa dočasne práceneschopný zamestnanec zdržiava na mieste určenom počas dočasnej pracovnej neschopnosti, pričom zamestnávateľ má právo vykonať túto kontrolu v obydlí zamestnanca s jeho súhlasom alebo na mieste kde je predpoklad, že sa dočasne zdržiava. Vychádzajúc z premisy, že zamestnanec má právo na ochranu tak súkromného, ako aj rodinného života, je oprávnenie zamestnávateľa takto kontrolovať zamestnanca podmienené rešpektovaním zásady proporcionality, v zmysle ktorej je zásah zamestnávateľa do práva zamestnanca na ochranu jeho súkromia obmedzené dodržiavaním miery, ktorá je nevyhnutná na dosiahnutie uvedeného cieľa a musí mať oporu v zákone. V danom prípade je právny základ takéhoto zásahu upravený práve v citovanom ustanovení zákona.

Diskutovanou témou je možnosť zamestnávateľa **zaznamenať telefonické hovory svojich zamestnancov**,[8] ktorá sa realizuje na jeho telekomunikačnom zariadení. Obsah takejto komunikácie požíva ochranu podľa článku 8 ods. 1 Dohovoru,[9] ako aj ústavnú ochranu.[10]

[8] K odpočúvaniu podrobnejšie pozri Čentéš, J.: Odpočúvanie – procesnoprávne a hmotnoprávne aspekty. Bratislava: C. H. Beck, 2012, 272 s.

[9] Pozri napr. Kmec, J., Kosář, D., Kratochvíl, J., Bobek, M.: Evropská úmluva o lidských právech. Komentář. 1. vydání. Praha: C. H. Beck, 2012, 1687 s., Szczechowicz K., Orłowska- Zielińska B.: Chosen aspects of the protection of private communication in legal systems and the influence of the European Court of Human Rights jurisdiction on their formation by the application of procedural telephone interception, Studia Prawnoustrojowe, Wydawnictwo UWM, Olsztyn 2012, 318 s.

[10] Pozri napr. Drgonec, J.: Právo na súkromie podľa Ústavy Slovenskej republiky. Časopis pro právní vědu a praxi, 2000, ročník VIII., č. 2, s. 203 – 212. Filip, J.: K otázce ústavní ochrany společnosti a státu de lege lata a de lege ferenda. Časopis pro právní vědu a praxi, II., 1996, č.4, s. 631 – 634. Svák, J.: Zásady a tendencie práva na súkromie. Justičná revue, 52, 2000, č. 11, s. 1199 – 1215. Holländer, P.: Základy všeobecné státovědy, 2. rozšírené vydanie. Plzeň: Aleš Čeněk, 2009, 364 s.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Zamestnávateľ nie je oprávnený zaznamenať telefonické hovory zamestnancov bez toho, aby ich na to vopred neupozornil, a to ani v prípade, že údaje v týchto hovoroch oznamované sa týkajú jeho záujmov. Tento záver možno podporiť aj rozhodnutiami Európskeho súdu pre ľudské práva, z ktorej vyplýva, že telefonické hovory uskutočnené z pracoviska môžu byť zahrnuté v pojmoch „súkromný život" a ,,korešpondencia" podľa článku 8 ods. 1 Dohovoru[11] a že odpočúvanie telefonických hovorov zamestnanca zamestnávateľom je neprípustné, ak nebol zamestnanec upozornený, že hovory vedené v internom komunikačnom systéme zamestnávateľa podliehajú odpočúvaniu, a rozumne – oprávnene očakával pri týchto hovoroch súkromie (reasonable expectation of privacy).[12] Ďalej Európsky súd pre ľudské práva zaujal stanovisko, že ,,*telefonický hovor nestráca svoj súkromný charakter tým, že sa jeho obsah týka alebo môže týkať verejného záujmu*."[13] Ak platí uvedený záver pre telefonické hovory týkajúce sa svojím obsahom verejného záujmu, potom obdobne platí aj pre telefonické hovory, ktorých obsah sa týka alebo môže týkať súkromia záujmu inej osoby (napr. zamestnávateľa).[14]

K uvedenému problému možno uviesť názor Heleny Barancovej podľa ktorej odpočúvanie telefonických hovorov zamestnanca by bolo možné len so súhlasom; a to nielen zamestnanca, ale aj so súhlasom tretej osoby, s ktorou zamestnanec telefonuje.[15] Z uvedeného možno vyvodiť právny záver, že odpočúvanie telefonických hovorov zamestnanca bez splnenia týchto podmienok zamestnávateľom je neprípustné a v rozpore s článkom 8 ods. 1 Dohovoru, a to bez ohľadu na charakter hovoru (súkromný alebo služobný).

Ďalej možno uviesť, že rozšírenú ochranu Dohovoru požíva zamestnanec (policajt), ktorého hovory zo služobného telefónu z pracoviska odpočúva zamestnávateľ, ktorým je orgán verejnej moci (polícia). V prípade, ak policajt nie je upozornený o odpočúvaní týchto hovorov zo strany zamestnávateľa môže sa domáhať ochrany podľa článku 8 ods. 1 a 2 Dohovoru.

[11] Coplandová v. Spojené kráľovstvo z 3. apríla 2007.
[12] Halfordová v. Spojené kráľovstvo z 25. júna 1997.
[13] A. v. Francúzsko z 23. novembra 1993. In: Čapek, J.: Z rozhodnutí Evropského soudu a Evropské komisie pro lidská práva (Ochrana soukromného a rodinného života, obydlí a korespondence)– část VII; Právní praxe, r. XLIII., 1995, č. 7, s. 430-432.
[14] Pozri odôvodnenie R ČR 39/1999, s. 334.
[15] Barancová, H.: Monitorovanie zamestnancov a ochrana súkromného života v judikatúre európskych súdov. In: Justičná revue, 63, 2011, č. 3, s. 340.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

V takomto prípade policajt rozumne – oprávnene očakáva súkromie. Telefónne spojenie prostredníctvom pevnej siete (napr. služobné telefóny) spadajú pod pojmy ,,súkromný život" a ,,korešpondencia" podľa článku 8 ods. 1 Dohovoru. V prípade, ak orgán verejnej moci odpočúva takéto hovory jedná sa o ,,zásah verejným orgánom" podľa článku 8 ods. 2 Dohovoru.[16]

Od tohto prípadu treba odlíšiť situáciu keď operačný dôstojník polície zavolal na domácu telefónnu stanicu príslušníka polície, ktorý mal tzv. dosažiteľnosť, teda vykonával plnohodnotné povinnosti vyplývajúce zo služobného pomeru príslušníka polície, pričom tento hovor bol políciou zaznamenaný na technické zariadenie, bez súhlasu príslušníka polície. Následne nahrávka tohto rozhovoru sa použila v trestnom konaní ako dôkaz. V tejto veci podal ústavnú sťažnosť obvinený (sťažovateľ), ktorého rozhovor bol zaznamenaný, pričom sa domáhal, aby Ústavný súd ČR zakázal okresnému súdu vykonať dôkaz prehratím záznamu telefónneho hovoru a navrhol, aby tento záznam bol vyradený zo spisu a aby bol zničený.

Ústavný súd ČR posúdil sťažnosť ako zjavne neopodstatnenú a dospel k záveru, že prítomnosť zvukového záznamu v spise a jeho vykonane ako dôkazu nezasahujú do tých základných práv sťažovateľa, ktoré namietal.[17] Ústavný súd ČR svoj záver odôvodnil tým, že ,,*právo na ochranu pred neoprávnenými zásahmi do súkromného a rodinného života sa vzťahuje iba na zásahy do súkromnej a rodinnej sféry, v ktorej jednotlivec prejavuje svoju osobnosť slobodne a autonómne. V tejto sfére sa však jednotlivec neocitá za situácie, v ktorej, hoci v rodinnom alebo súkromnom prostredí vystupuje alebo plní funkcie verejného charakteru a obzvlášť povinnosti vyplývajúce zo služobného pomeru príslušníka polície.*" Postavenie jednotlivca v postavení príslušníka polície pri výkone služobného pomeru sa výrazne líši od jeho právneho postavenia ako súkromnej osoby. Z podstaty služobného pomeru vyplýva, že príslušník je pri výkone služby v postavení podriadeného voči nadriadenému, a v takejto pozícii sa musí podriadiť príkazom nadriadeného, s ktorými má povinnosť sa zoznámiť. Sťažovateľ bol informovaný o tom, že hovor uskutočnený s operačným strediskom polície je zaznamenaný na

[16] Halfordová v. Spojené kráľovstvo z 25. júna 1997.
[17] I. ÚS ČR 28/04.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

technické zariadenie. Z uvedeného možno vyvodiť, že sa jednalo o služobný hovor, obligatórne zaznamenávaný, čo vylučuje sťažnosť proti zásahom do súkromnej sféry jednotlivca.

Pokiaľ mal sťažovateľ v dobe uskutočnenia rozhovoru tzv. dosažiteľnosť, t. j. vykonával služobné povinnosti mimo úradovňu v súkromí, poskytol svoju súkromnú telefónnu stanicu k dispozícii k výkonu služobných úkonov. Z uvedeného dôvodu dal súhlas k tomu, aby sa na komunikáciu uskutočňovanú na súkromnej stanici s dispečingom polície vzťahoval režim ako na iné stanice slúžiace na výkonu úloh polície. V takomto rozsahu sám vedome obmedzil rozsah ochrany svojho súkromia. Takúto vedomosť možno vyvodzovať tiež z obsahu komunikácie iných príslušníkov polície, podriadených v služobnom pomere sťažovateľovi, ktoré boli vedľa tejto komunikácie sťažovateľa zaznamenané a z ktorých vyplýva, že si boli vedomí skutočnosti, že obsah komunikácie je zaznamenávaný, a preto odkazovali na súkromné mobilné telefónne spojenie. Pokiaľ títo podriadení boli uzrozumení so záznamami komunikácie, je preto potrebné takúto vedomosť prisudzovať sťažovateľovi.

Pre úplnosť možno uviesť, že odlišne by sa posudzovala situácia v prípade, keby sťažovateľ zo svojho domova nevykonával povinnosti vyplývajúce zo služobného pomeru (napr. nemal by tzv. dosažiteľnosť) a bolo by mu na súkromnú telefónnu stanicu volané z operačného strediska polície, ktoré komunikáciu zaznamenáva. Takýto rozhovor by zrejme nesplňoval charakter služobného rozhovoru, napriek tomu, že by sa obsahovo týkal činnosti príslušníkov polície.

Diskutovanou otázkou je tiež **monitorovanie internetovej elektronickej pošty (e-mailov)** zamestnanca, zo strany zamestnávateľa. Podľa Pavla Matesa zamestnávateľ môže monitorovať počet e-mailov, požadovať, aby zamestnanci minimalizovali vybavovanie súkromných záležitostí na pracovisku a zakázať, aby elektronické prostriedky boli používané na nedovolené ciele. O tom, že tak bude konať, má zamestnanca vopred jasne informovať. V žiadnom prípade však nie je oprávnený čítať obsah odovzdávaných správ. Tento záver platí ako o textoch odoslaných a prijatých, ako aj tých, ktorých kópia zostáva na serveri.[18]

[18] Mates, P.: Ochrana soukromí v správním právu. 2. aktualizované a podstatně přepracované vydání, Linde, Praha, s. 149-150.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

V prípade pracovnej e-mailovej korešpondencie zamestnanca je zamestnávateľ oprávnený ju prečítať v tom prípade, ak nie je zamestnanec aktuálne prítomný na pracovisku a omeškanie by mohlo zasiahnuť do majetkovej sféry zamestnávateľa. V prípade, ak zamestnávateľ (vedúci zamestnanec) otvorí e-mail, ktorý nemohol byť identifikovaný ako súkromný, a napriek tomu to tak je, je povinný, ak zistí, že ide o súkromný e-mail, čítanie ukončiť. Akékoľvek ďalšie čítanie alebo otváranie e-mailu, ktorý mohol a mal byť identifikovaný ako súkromný, je porušením listového tajomstva. V súvislosti s neoprávneným zásahom do súkromia zamestnanca zo strany zamestnávateľa možno konštatovať absenciu ustanovení zakotvujúcich zodpovednosť zamestnávateľa v Zákonníku práce. V takomto prípade možno uplatniť občianskoprávne ustanovenie bez akéhokoľvek vzťahu k pracovnému právu.

Pri zásahoch do súkromia zamestnanca zo strany zamestnávateľa dochádza k nakladaniu s informáciami, ktoré môžu mať povahu osobných údajov, týkajúcich sa či už zamestnanca alebo tretej osoby. Zákonník práce neustanovuje, či zamestnávateľ je oprávnený pri narušení súkromia zamestnanca zasiahnuť aj do iných práv, napríklad práva na ochranu osobných údajov. Podľa Barancovej dochádza k zásahu do osobnostných práv zamestnanca z hľadiska jeho oprávnených záujmov ochrany osobných údajov najčastejšie už v rámci predzmluvných vzťahov. Zamestnávateľ nezriedka kedy žiada od budúceho zamestnanca uviesť bližšie osobné údaje nielen o sebe, ale aj o jeho rodine, rodičoch, manželovi a deťoch. Zákonník práce zakazuje vyžadovať od fyzickej osoby uchádzajúcej sa o zamestnanie informácie, ktorými by sa mohla poškodiť osobnosť uchádzača o zamestnanie.[19] Vzhľadom na okolnosť, že zamestnávateľ sa pri zásahoch do súkromia zamestnancov spravidla stáva správcom osobných údajov, jeho činnosť je okrem pracovnoprávnych predpisov regulovaná aj právnymi predpismi na úseku ochrany osobných údajov – konkrétne zákonom o ochrane osobných údajov. Podľa odbornej literatúry najdôležitejšou povinnosťou, ktorú bude potrebné splniť ešte pred začatím vykonávania zásahov do súkromia zamestnanca, je získať súhlas od zamestnanca. Zákonník práce uvedenú povinnosť neustanovuje. Táto povinnosť vyplýva zo zákona o ochrane osobných údajov. Nebolo by ju možné nahradiť ani súhlasom, ktorý zamestnanec dáva, pri uzatváraní pracovnej zmluvy, aby sa mohli jeho údaje spracúvať na personálne účely.

[19] Barancová, H., Schronk, R.: Pracovné právo, Bratislava 2013, Sprint 2, ISBN: 978-80-89393-97-8, s. 117.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Došlo by tak k porušeniu zásady proporcionality, keďže osobné údaje možno spracúvať len na vopred určený účel. Takisto možno zvýrazniť potrebu jasného, jednoznačného a konkrétneho vymedzenia súhlasu so spracovaním osobných údajov zamestnanca.

Na základe uvedených skutočností možno na tomto mieste zaujať tento čiastkový záver. Zamestnávateľ nie je oprávnený bez vážnych dôvodov narúšať súkromie svojho zamestnanca, pri zásahoch do súkromia zamestnanca je zamestnávateľ povinný vopred upozorniť zamestnanca na túto možnosť a oznámiť mu rozsah kontroly. Zároveň je povinný so zástupcami zamestnávateľov prerokovať rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania. Z týchto dôvodov by narušenie súkromia nemalo obmedzovať zamestnanca, čo do rozsahu a intenzity prijatých opatrení viac, ako je nevyhnutne potrebné. V rámci uvedeného je hodnotenie úlohy pracovnoprávnej legislatívy pri úprave zásahov do súkromia zamestnanca, vychádzajúc z analyzovanej novelizácie Zákonníka práce, účinnej od 1.1.2013 pozitívna a posilňujúca zákonnú ochranu súkromia zamestnancov.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2 OCHRANA OSOBNÝCH ÚDAJOV ZAMESTNANCA PODĽA NARIADENIA GDPR

Systém ochrany osobných údajov v rámci Európskej únie (ďalej len „**EÚ**“) pramení z toho, že právo na ochranu osobných údajov je chránené ako základné ľudské právo a sloboda v rámci článku 8 Charty základných práv EÚ. V roku 2016 prešla legislatíva na ochranu osobných údajov zásadnou zmenou, keď staršiu a v mnohých členských štátoch nesprávne transponovanú právnu úpravu nahradila nová. Túto novú právnu úpravu tvorí:

- GDPR; a
- Smernica o presadzovaní práva.[20]

GDPR predstavuje **všeobecný právny** rámec ochrany osobných údajov v EÚ a vzťahuje sa na akékoľvek spracúvanie osobných údajov. „Toto nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.“[21] Nezáleží či osobné údaje spracúva orgán verejnej moci alebo súkromný subjekt, GDPR sa na nich vzťahuje v zásade rovnakým spôsobom. Uplatňuje sa teda aj v prípade spracúvania osobných údajov zamestnanca zamestnávateľom.

Pri analýze a výklade GDPR považujeme za vhodné poukázať na niekoľko praktických usmernení. Samotný text GDPR je na mnohých miestach všeobecný a používa vágne pojmy, ktoré v nariadení nie sú priamo definované (napr. vysoké riziko alebo primerané opatrenia). Nie je to však nevyhnutné negatívum právneho predpisu, skôr výhoda, ktorá odzrkadľuje rôznorodosť a vhodnosť interpretácie v rôznych podmienkach a rôznych situáciách.

Pri interpretácii textu GDPR je tak možné využiť viacero relevantných pomôcok. Prvou z nich sú úvodné ustanovenia (recitály) GDPR, ktoré precizujú samotný text Nariadenia a často

[20] Pre úplnosť považujeme za potrebné dodať, že EÚ prijala aj špecifický právny rámec spracúvania osobných údajov pre inštitúcie EÚ - Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES. Toto nariadenie je z hľadiska predmetu tejto Analýzy úplne irelevantné.

[21] GDPR, článok 2

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

poskytujú hlbší výklad niektorých ustanovení. Druhou pomôckou sú názory a usmernenia Výboru na ochranu údajov (*European Data Protection Board* – EDPB). Ide o samostatný orgán na úrovni EÚ, ktorý vydáva *soft law* k jednotlivých ustanoveniam GDPR. Predchodcom EDPB bola Pracovná skupina článku 29 (*Article 29 Data Protection Working Party* – ***WP29***) a jej usmernenia a stanoviská sú stále použiteľné aj v kontexte novej právnej úpravy. Opomenúť nemožno ani stanoviská Európskeho dozorného úradníka pre ochranu údajov (*European Data Protection Supervisor* – ***EDPS***), ktorý pravidelne publikuje svoje názory na aktuálne otázky ochrany osobných údajov. Stanoviská a usmernenia poskytujú aj konkrétne národné dozorné orgány na úseku ochrany osobných údajov a v slovenskej právnej realite tak nemožno úplne ignorovať dokumenty publikované Úradom na ochranu osobných údajov Slovenskej republiky. Úrad na ochranu osobných údajov SR zároveň rozhoduje ako dozorný orgán podľa GDPR a tým pádom sú cenným zdrojom aj jeho rozhodnutia.

GDPR v tomto kontexte prinieslo aj viaceré zmeny z hľadiska procesu, činnosti a funkcii dozorných orgánov. Jednou z noviniek sú aj požiadavky na konzistentné konanie dozorných orgánov vrátane mechanizmu konzistentnosti. Článok 51 ods. 2 GDPR ustanovuje: *„Každý dozorný orgán prispieva ku konzistentnému uplatňovaniu tohto nariadenia v celej Únii.“* Podľa komentátorov ide o silnú deklaráciu pre požiadavku konformného rozhodovania dozorných orgánov v EÚ.[22] To prirodzene nevylučuje autonómiu rozhodovania dozorných orgánov v prípadoch, keď sa skutkový stav alebo aplikácia národného práva týka špecificky právneho poriadku konkrétneho členského štátu. Ide teda o situácie, v ktorých si členské štáty mohli pravidlá na ochranu osobných údajov upraviť samé ako napríklad vyváženie ochrany osobných údajov so slobodou prejavu alebo spracúvanie národných identifikátorov.

Predmetná deklarácia je ešte viac zvýraznená prostredníctvom požiadaviek na spoluprácu a mechanizmu konzistentnosti. Článok 63 GDPR v tomto smere špecifikuje, že *„S cieľom prispievať ku konzistentnému uplatňovaniu tohto nariadenia v celej Únii dozorné orgány spolupracujú navzájom a v relevantných prípadoch s Komisiou prostredníctvom mechanizmu konzistentnosti, ako sa stanovuje v tomto oddiele.“* Mechanizmus konzistentnosti má viaceré

[22] HIJMANS, H. Article 51. In KUNER, CH. a kol. *The EU General Data Protection Regulation (GDPR). A commentary*. Oxford University Press, 2020.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

podoby. V prvom rade sú dozorné orgány ho povinné využiť v prípade, ak ich rozhodnutia bude mať právne účinky (ovplyvnia väčší počet dotknutých osôb) vo viacerých členských štátoch EÚ prípadne, ak sa Výbor na ochranu alebo iný dozorný orgán domnieva, že takýto efekt nastane. V danom prípade Výbor na ochranu údajov vydá rozhodnutie, ktoré prípad vyrieši. V druhom rade konzistentnosť zabezpečuje aj rozhodovanie kompetenčných sporov zo strany daného Výboru. Všetky menované mechanizmy a ustanovenia či už priamo alebo nepriamo vyžadujú, aby dozorné orgány v členských štátoch EÚ uplatňovali GDPR konzistentne. To prakticky znamená, že v podobných prípadoch by mali rozhodovať podobným spôsobom. Dozorné orgány majú navyše k dispozícii databázu rozhodnutí iných členských štátov a komunikačné línie na zabezpečenie konzistentnosti. Je pravda, že rozhodnutie dozorného orgánu v inom členskom štáte nie je na Slovensku právne záväzné, avšak môže predstavovať veľmi silný argument v prospech určitého výkladu GDPR spolu so zvýraznením požiadaviek na konzistentnosť uvedených v GDPR. V rámci tejto analýzy tak budeme zohľadňovať aj niektoré rozhodnutia zahraničných dozorných orgánov, ktoré môžu predstavovať pomôcku pri aplikácií GDPR v slovenských podmienkach.

Ďalším interpretačným zdrojom sú rozhodnutia SDEÚ a ESĽP pri výklade relevantných článkov Dohovoru, Charty, ale aj priamo Smernice 95/46/EHS či GDPR.

2.1 SUBJEKTY PARTICIPUJÚCE V SYSTÉME OCHRANY OSOBNÝCH ÚDAJOV

Subjekty participujúce v systéme ochrany osobných údajov možno derivovať z osobnej pôsobnosti GDPR. Nariadenie síce neobsahuje výslovne vymedzené ustanovenie s názvom „osobná pôsobnosť," avšak v rámci právneho textu definuje a upravuje rôzne povinnosti súvisiace s aktérmi spracúvania osobných údajov. Ak určitá entita spĺňa požiadavky materiálnej[23] a teritoriálnej pôsobnosti[24] GDPR, je vhodné pristúpiť ku skúmaniu, v akej pozícií sa vlastne nachádza. V tomto kontexte GDPR definuje dvoch kľúčových aktérov spracúvania osobných údajov – prevádzkovateľa (*controller)* a sprostredkovateľa (*processor)* osobných údajov. Správne definovanie entity je osobitne dôležité s ohľadom na distribúciu zodpovednosti za súlad s legislatívnymi požiadavkami na spracúvanie osobných údajov.

[23] Článok 2, GDPR.
[24] Článok 3, GDPR.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Okrem vyššie uvedených pojmov GDPR rozlišuje ešte dotknutú osobu, príjemcu a tretiu stranu.

2.1.1 Prevádzkovateľ

Prevádzkovateľ je v GDPR legálne definovaný ako „fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov.“[25] EDPB vydal usmernenie[26] k pojmom prevádzkovateľ a sprostredkovateľ. Dané usmernenie implicitne rešpektuje aj novšia judikatúra Súdneho dvora Európskej únie (ďalej len „SDEÚ“) k výkladu daného pojmu.[27]

EDPB vymedzuje päť osobitných prvkov definície prevádzkovateľa: (i) fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt; (ii) ktorý sám alebo spoločne s inými; (iii) určí; (iv) účely a prostriedky; (v) spracúvania osobných údajov.[28] Najdôležitejšie prvky danej definície analyzujeme nižšie.

Prvým aspektom definície je určenie entity, ktorá osobné údaje spracúva. WP29 zvýrazňuje, že v tomto kontexte je potrebné skúmať zaužívané inštitúty súkromného a verejného práva, ktoré by nás mali nasmerovať k finálnemu určeniu konkrétnej entity. Za prevádzkovateľa by mala byť považovaná spoločnosť alebo orgán, nie špecifická osoba v rámci ich štruktúr.[29] SDEÚ v prípade *Google Spain* uviedol, že *„založenie takejto inštitúcie na území členského štátu predpokladá účinné a skutočné vykonávanie činnosti prostredníctvom stabilných dohôd [prostredníctvom stálej prevádzkarne – neoficiálny preklad]“ a že „právna forma takejto*

[25] Článok 4 (7), GDPR.
[26] European Data Protection Board. Guidelines. 07/2020 on the concepts of controller and processor in the GDPR. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.
[27] Pozri napr. Rozsudok Súdneho dvora zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16.
[28] European Data Protection Board Guidelines. 07/2020 on the concepts of controller and processor in the GDPR. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en, s. 9.
[29] Tamže, s. 10.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

inštitúcie, či je to pobočka, alebo dcérska spoločnosť s právnou subjektivitou, nie je určujúcim činiteľom".[30] Túto požiadavku v súčasnosti odzrkadľuje Recitál 22 GDPR.[31]

Druhý aspekt reflektuje, či subjektov, ktoré možno považovať za prevádzkovateľov je viacero alebo je len jeden. Tejto problematike sa osobitne venujeme v časti „spoloční prevádzkovatelia" nižšie.

Najdôležitejším aspektom definície je určenie účelov a prostriedkov spracúvania osobných údajov. EDPB predmetný aspekt diferencuje na problematiku „určenia" a „účelov a prostriedkov" spracúvania osobných údajov.

Určenie účelov je potrebné vnímať v kontexte inštitútu prevádzkovateľa, ktorý je dynamický a funkčný, čo v praxi znamená posudzovanie faktických okolností a nie iba formálneho splnenie niekoľkých kritérií.[32] Požiadavka „určenia" účelov a prostriedkov spracúvania osobných údajov môže vyplávať z troch legitímnych zdrojov. EDPB konkrétne uvádza (i) explicitnú požiadavku ustanovenú právom, (ii) implicitnú požiadavku ustanovenej právom alebo (iii) faktického vplyvu.[33] Pri explicitnej požiadavke upravenej v právnom poriadku pôjde zväčša o situácie, keď právna norma obsahuje obligáciu zbierať a spracúvať osobné údaje.[34] Implicitná požiadavka na spracúvania osobných údajov spočíva v prirodzenom súvise medzi určitou entitou a spracúvaním osobných údajov, čo je osobitne dôležité v prípadoch, keď právny predpis priamu obligáciu neobsahuje, ale je nepriamo vyplýva zo znenia legislatívneho

[30] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12.
[31] Recitál 22, GDPR: „Každé spracúvanie osobných údajov v kontexte činností prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Únii by sa malo vykonávať v súlade s týmto nariadením bez ohľadu na to, či sa samotné spracúvanie uskutočňuje v Únii. Prevádzkareň znamená efektívny a skutočný výkon činnosti prostredníctvom stálych dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom."
[32] European Data Protection Board Guidelines. 07/2020 on the concepts of controller and processor in the GDPR. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en, s. 10 - 11.
[33] Tamže.
[34] Ako príklad zo slovenského právneho poriadku možno uviesť postavenie advokátov v zmysle § 18 ods. 6 zákona č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov: *„Advokát spracúva osobné údaje klientov a iných fyzických osôb v rozsahu nevyhnutnom na účely výkonu advokácie v súlade s týmto zákonom a s osobitným predpisom. Advokát má pri spracúvaní osobných údajov v zmysle prvej vety tohto odseku postavenie prevádzkovateľa podľa osobitného predpisu."*

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

textu.[35] Tretím zdrojom postavenia prevádzkovateľa môžu byť faktický vplyv a okolnosti daného spracúvania osobných údajov. V tomto kontexte EDPB uvádza zmluvné podmienky ako faktor, ktorý je potrebné brať do úvahy, avšak nie absolútne, nakoľko rozhodujúci je reálny stav a nie ustanovenia v zmluve. Ďalšie faktory, ktoré je možné posudzovať sú stupeň kontroly v rámci spracovateľských operácii, „image" vytvorený voči dotknutým osobám či primerané očakávaní dotknutých subjektov.[36] Subjekt, ktorý má nulový faktický alebo právny vplyv na určenie účelov a prostriedkov spracovania osobných údajov nemôže byť považovaný za prevádzkovateľa.

Určenie účelu spracovania je výsadou prevádzkovateľa. Účel možno zjednodušene vymedziť ako cieľ spracovateľskej operácie. Určenie účelov a prostriedkov spracúvania teda reflektuje „prečo" a „ako" budú osobné údaje spracúvané. Esenciou pri analýze daného faktora je úroveň detailov pri predmetnom determinovaní.[37] Prostriedky spracúvania osobných údajov zahŕňajú technické a organizačné aspekty spracúvania osobných údajov. Môže ísť aj o určenie toho, aké údaje sa budú spracúvať, aké tretie strany budú mať k údajom prístup či určenie dôb uchovávania.[38] Prostriedky spracúvania osobných údajov a ich určenie môže byť delegované na sprostredkovateľov, ak hovoríme o organizačných a technických otázkach (software, hardware).

Problematiku (spoločného) vymedzenia účelu ilustruje známy prípad vo veci SWIFT. Spoločnosť SWIFT figurovala ako sprostredkovateľ pri spracúvaní osobných údajov európskych bankových inštitúcií. Zároveň ale bez príkazu európskych bánk sprístupňovala údaje o dotknutých osobách v Európe Ministerstvu financií v Spojených štátoch amerických.

[35] Ako príklad možno uviesť spracúvanie osobných údajov zamestnávateľom v zmysle zákona č. 311/2001 Z. z. Zákonníka práce.
[36] European Data Protection Board Guidelines. 07/2020 on the concepts of controller and processor in the GDPR. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en, s. 12.
[37] Tamže, s. 13.
[38] Tamže, s. 13 - 14.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

WP29 (Article 29 Data Protection Working Party, predchodca EDPB) vo svojom názore[39] vyslovila záver, že spoločnosť SWIFT na seba delegovala právomoci prevádzkovateľa (poskytnutím údajov o dotknutých osobách) a stala sa tak spoločným prevádzkovateľom spolu s bankovými inštitúciami, ktoré na druhej strane značne zanedbali dohľad nad aktivitami svojho sprostredkovateľa.

2.1.2 Spoloční prevádzkovatelia

Ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi.[40] S inštitútom spoločných prevádzkovateľov rátala už síce Smernica 95/46/ES v intenciách usmernenia WP29, avšak výslovne zakotvenie daného inštitútu upravuje až GDPR. Nie je dôležitá úroveň prepojenia spoločných prevádzkovateľov (od spoločného zdieľania výkonu všetkých spracovateľských operácii až po zdieľanie výkonu len jednej spracovateľskej operácie).[41] Typickým príkladom spoločných prevádzkovateľov je vedenie databázy dlžníkov viacerými entitami napr. vo finančnom sektore. Na tomto mieste je ale potrebné upozorniť na rozdiel medzi spoločnými prevádzkovateľmi a prenosom osobných údajov (napr. cestovná agentúra, ktorá pošle dáta svojich zákazníkom leteckej spoločnosti a hotelovému zariadeniu). Iná by bola situácia, ak by cestovná agentúra, hotel a letecká spoločnosť založila spoločnú databázu manažmentu rezervácii. V takomto prípade by sa jednalo o spoločných prevádzkovateľov.[42]

Napriek výslovnému zakotveniu predmetného inštitútu v GDPR viacerí autori poukazujú na to, že špecifické otázky týkajúce sa alokácie zodpovednosti sú stále predmetom nejasností a diskusií.[43]

2.1.3 Sprostredkovateľ

[39] Article 29 Data Protection Working Party. Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). 2006. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf.
[40] Článok 26 ods. 1, GDPR.
[41] European Data Protection Board Guidelines. 07/2020 on the concepts of controller and processor in the GDPR. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en, s . 17 a nasl.
[42] Tamže, s. 20 – 21.
[43] Pozri napr. VAN ALSENOY, Brendan: Liability under EU Data Protection Law. *In 7 (2016) JIPITEC 271*.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Sprostredkovateľ je v zmysle článku 4 bodu 8 GDPR „fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.“ Na kvalifikovanie entity ako sprostredkovateľa musia byť kumulatívne splnené dva atribúty. V prvom rade musí ísť o odlišnú entitu od prevádzkovateľa. Druhým kritériom je, že spracúvanie osobných údajov sa vykonáva v mene prevádzkovateľa.[44] Inštitút sprostredkovateľa reflektuje delegáciu resp. poverenie spracúvať osobné údaje na iné entity. Do spracúvania osobných údajov je zároveň možné zapojiť aj ďalších sprostredkovateľov (sub-sprostredkovateľov). Sprostredkovateľ to však môže urobiť iba so súhlasom prevádzkovateľa.[45]

2.1.4 Iné subjekty

Okrem kľúčových aktérov spracúvania osobných údajov v podobe prevádzkovateľa a sprostredkovateľ upravuje GDPR definíciu a postavenie ďalších troch entít.

V prvom rade GDPR na mnohých miestach v legislatívnom texte ustanovuje práva a povinnosti pre dotknuté osoby. GDPR dotknutú osobu definuje ako identifikovanú alebo identifikovateľnú fyzickú osobu, ktorej sa osobné údaje týkajú.[46] Inými slovami, dotknutá osoba je osoba, ktorej osobné údaje sú spracúvané ako napr. bežný užívateľ sociálnej siete, zamestnanec z pohľadu zamestnávateľa alebo zákazník alebo klient elektronického obchodu či služby.

Ďalším pojmom, ktorý GDPR upravuje je príjemca. V zmysle definície je príjemca „fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou.“[47] Zároveň GDPR obsahuje aj negatívnu definíciu príjemcu týkajúceho sa orgánu verejnej moci pri výkone svojich oprávnení a úloh.[48]

---

[44] European Data Protection Board Guidelines. 07/2020 on the concepts of controller and processor in the GDPR. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en, s. 24.
[45] Článok 28 ods.4, GDPR.
[46] Viď článok 4 bod 1, GDPR.
[47] Článok 4 bod 9, GDPR.
[48] Článok 4 bod 8, GDPR: „Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.“

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Príjemcom tak napr. môže byť sprostredkovateľ alebo poverený zamestnanec prevádzkovateľa.

Posledným pojmom do mozaiky osobnej pôsobnosti GDPR je tretia strana. Tretia je strana je definovaná primárne prostredníctvom negatívnej enumerácie: *„Tretia strana...je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.“*[49]

2.1.4.1 Zamestnanci ako dotknuté osoby

Považujeme za vhodné uviesť, že GDPR síce pristupuje ku všetkým subjektom v súlade so zásadou rovnosti, ale zároveň priamo či nepriamo niektoré kategórie dotknutých osôb zaradzuje medzi tzv. zraniteľné dotknuté osoby (*vulnerable data subjects*). Medzi takéto osoby môžeme zaradiť deti a taktiež zamestnancov v súvislosti s niektorými spracovateľskými operáciami a inštitútmi. Predovšetkým možno spomenúť sledovanie na pracovisku, evidenciu dochádzky alebo vyžadovanie súhlasu.

Základné postuláty ochrany súkromia a osobných údajov upravuje Zákonník práce.[50] Článok 11 ustanovuje, že „Zamestnávateľ môže o zamestnancovi zhromažďovať len osobné údaje **súvisiace s kvalifikáciou a profesionálnymi skúsenosťami** zamestnanca a údaje, ktoré môžu byť **významné** z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával.“ V tomto princípe je zvýraznená nevyhnutnosť spracúvania údajov o zamestnancovi zo strany zamestnávateľa a potreba vyvažovania práv dotknutých strán. Zároveň Zákonník práce upravuje aj generálnu klauzulu, týkajúcu sa monitorovania zamestnancov.[51]

[49] Článok 4 bod 10, GDPR.
[50] Zákon č. 311/2001 Z. z. Zákonník práce.
[51] § 13 ods. 4 Zákonníka práce: „Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje, vykonáva záznam telefonických hovorov uskutočňovaných technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronickú poštu odoslanú z pracovnej elektronickej adresy a doručenú na túto adresu bez toho, aby ho na to vopred upozornil. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.“

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2.1.5 Špecifické subjekty

2.1.5.1 Oprávnená osoba

Staršia slovenská právna úprava operovala aj s termínom oprávnená osoba. V zmysle § 4 ods. 2 písm. e) sa za oprávnenú osobu považovala *„každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa § 21.“*[52]

Súčasná legislatíva už tento termín nepozná. V kontexte GDPR by sú oprávnenými osobami príjemcovia osobných údajov, vo veľmi špecifických prípadoch tretie strany.

2.1.5.2 Zodpovedná osoba (DPO)

Inštitút zodpovednej osoby (*Data protection officer*) nie je minimálne v slovenskom právnom poriadku nový, nakoľko poverenie zodpovednej osoby upravoval už zákon č. 122/2013 Z. z. o ochrane osobných údajov. Jeho podstata spočíva vo vymenovaní poverenej fyzickej alebo právnickej osoby vnútri organizácie alebo aj externe, ktorá dohliada a monitoruje spracúvanie osobných údajov v konkrétnej organizácii. Napriek tomu, že v názve tejto funkcie je slovo *„zodpovedná“*, neznamená to, že táto osoba je zodpovedná za spracúvanie osobných údajov v zmysle administratívnoprávnej, občianskoprávnej alebo trestnoprávnej zodpovednosti. S určitým nadsadením možno konštatovať, že skôr ide o mentora alebo kontrolný orgán v rámci organizácie. K inštitútu zodpovednej osoby vydal usmernenie aj WP29[53].

Kedy je prevádzkovateľ alebo sprostredkovateľ povinný dotknutú osobu vymenovať, upravuje článok 37 ods. 1 GDPR. V zmysle daných ustanovení táto povinnosť nastáva, ak:

- spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt s výnimkou súdov pri výkone ich súdnej právomoci;

[52] Zákon č. 122/2013 Z. z. o ochrane osobných údajov.
[53] Article 29 Data Protection Working Party. Guidelines on Data Protection Officers (‘DPOs’) Adopted on 13. December 2016 As last Revised and Adopted on 5. April 2017.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu alebo
- hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií údajov podľa článku 9 GDPR vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10 GDPR.

Hlavnou činnosťou v zmysle vyššie uvedených ustanovení sa myslí taká činnosť, ktorá je absolútne rozhodujúca pre činnosť danej organizácie.

Zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany údajov[54]. GDPR tak priamo nevyžaduje vykonanie odbornej skúšky alebo vzdelanie v odbore právo či informačná bezpečnosť.

Ak prevádzkovateľ alebo sprostredkovateľ zodpovednú osobu vymenujú, jej kontaktné údaje musia byť zverejnené a zároveň je potrebné danú osobu nahlásiť dozornému orgánu. Ak sa zodpovedná osoba nahlasuje Úradu na ochranu osobných údajov SR, je tak potrebné urobiť prostredníctvom špeciálneho formuláru zverejneného na webovom sídle dozorného orgánu[55].

Zodpovedná osoba musí mať nezávislé postavenie pri plnení svojich úloh. To prakticky znamená, že prevádzkovateľ alebo sprostredkovateľ je povinný zabezpečiť, aby zodpovedná osoba v súvislosti s plnením týchto úloh nedostávala žiadne pokyny. Zároveň zodpovednú osobu nesmú odvolať alebo postihovať za výkon jej úloh. Zodpovedná osoba podlieha priamo najvyššiemu vedeniu prevádzkovateľa alebo sprostredkovateľa[56].

Táto osoba musí byť riadnym spôsobom a včas zapojená do všetkých záležitostí, ktoré súvisia s ochranou osobných údajov a organizácia jej musí poskytnúť podporu a zdroje na zvyšovanie svojich odborných znalostí[57]. Zodpovedná osoba je kontaktným bodom pre dotknuté osoby,

[54] Článok 37 ods. 5 GDPR.
[55] Dostupné na https://dataprotection.gov.sk/uoou/sk/zo/register-zo (dostupné 1. 8. 2023).
[56] Článok 38 ods. 3 GDPR.
[57] Článok 38 ods. 1 a 2 GDPR.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ktoré si chcú uplatniť svoje práva v zmysle článkov 15 – 22 GDPR, pričom všeobecne je táto osoba viazaná povinnosťou zachovávať mlčanlivosť[58]. Nie je vylúčené, že zodpovedná osoba musí plniť aj iné úlohy v rámci organizácie, avšak za podmienky, že nedochádza ku konfliktu záujmov[59].

Z hľadiska úloh upravených v článku 39 možno povinnosti zodpovednej osoby rozdeliť do štyroch oblastí:

- **monitorovanie** – zodpovedná osoba monitoruje súlad s GDPR a inými právnymi predpismi v danej organizácii vrátane interných predpisov a taktiež vykonáva interné audity
- **poradenstvo** – zodpovedná osoba poskytuje na požiadanie poradenskú činnosť v oblasti ochrany osobných údajov organizácií a jej zamestnancom; osobitne možno zdôrazniť poradenskú činnosť pri vypracovaní posúdenia vplyvu na ochranu osobných údajov v zmysle článku 35 GDPR
- **vzdelávanie** – zodpovedná osoba obstaráva vzdelávanie zamestnancov organizácie, školí ich v danej oblasti a zvyšuje povedomie a odbornosť v danej oblasti
- **kontaktný bod** – zodpovedná osoba plní úlohu kontaktného miesta pre dotknuté osoby pri výkone ich práv a pre dozorný orgán pri spolupráci alebo predchádzajúcej konzultácii.

V kontexte pracovnoprávnych vzťahov je nutné poznamenať, že ak by zamestnávateľ v pozícii prevádzkovateľa mal iba tento jeden účel, nebolo by potrebné ustanoviť zodpovednú osobu. V praktickej rovine však prevádzkovatelia mávajú viacero účelov spracúvania osobných údajov. Z tohto dôvodu musia posúdiť, či nie sú v postavení orgánu verejnej moci alebo nevykonávajú ako hlavnú činnosť jednu z vyššie uvedených činností. Je nutné poznamenať, že monitorovanie zamestnancov prostredníctvom kontrolného mechanizmu zamestnávateľa nie je hlavnou náplňou akéhokoľvek prevádzkovateľa.

[58] Článok 38 ods. 4 a 5 GDPR.
[59] Článok 38 ods. 6 GDPR.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2.2 VYBRANÉ PRÁVA A POVINNOSTI ZAMESTNÁVATEĽA Z POHĽADU OCHRANY OSOBNÝCH ÚDAJOV

Prevádzkovatelia a sprostredkovatelia sú v zmysle GDPR kľúčové entity zodpovedné za spracúvanie osobných údajov a preto sa na nich vzťahuje niekoľko povinnosti. Za najvšeobecnejšiu formuláciu povinností možno považovať článok 24 ods. 1 GDPR: *„S ohľadom na povahu, rozsah,* kontext *a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb* ***prevádzkovateľ prijme vhodné technické a organizačné opatrenia****, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením.“* Táto povinnosť sa v praxi zabezpečuje prijatím interných dokumentov (napríklad interná politika ochrany osobných údajov alebo bezpečnostná politika) a implementovaním organizačných a technických opatrení pri práci s osobnými údajmi v organizácií. Predmetná povinnosť je dynamická a znamená, že v prípade prijatia vyššie uvedených opatrení je ich potrebné pravidelne posudzovať a aktualizovať. Nakoľko zamestnávatelia budú primárne v postavení prevádzkovateľov, tieto povinnosti je nevyhnutné aplikovať aj na nich.

Dôležitou povinnosť prevádzkovateľa je postup, ak sa rozhodne do spracúvania osobných údajov zapojiť sprostredkovateľa. „Ak sa má spracúvanie uskutočniť v mene prevádzkovateľa, prevádzkovateľ využíva len sprostredkovateľov poskytujúcich dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky tohto nariadenia a aby sa zabezpečila ochrana práv dotknutej osoby.“[60] Prakticky to znamená, že prevádzkovateľ si musí preveriť potenciálneho sprostredkovateľa a spracúvanie osobných údajov môže „zveriť“ iba organizácií, ktorá spĺňa určité kritéria. Osobitnou povinnosťou je uzatvorenie tzv. sprostredkovateľskej zmluvy so sprostredkovateľom v zmysle kritérií článku 28 ods. 3 GDPR. Ak teda zamestnávateľ využíva na spracúvanie osobných údajov sprostredkovateľa ako napríklad softvérovú firmu zabezpečujúcu manažment personalistiky a miezd, tieto požiadavky bude musieť naplniť.

[60] Článok 28 ods. 1 GDPR.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Z hľadiska zodpovednosti môžu byť za porušenie pravidiel na ochranu osobných údajov v zmysle GDPR braní na zodpovednosť aj prevádzkovateľ aj sprostredkovateľ. Vo vnímaní zodpovednosti tak nastala zásadná zmena oproti staršej legislatíve, na základe ktorej mohol byť zodpovedný iba prevádzkovateľ. Nové nariadenie umožňuje, aby bol za porušenie GDPR zodpovedný aj sprostredkovateľ a to buď priamym porušením jemu ustanovených povinností alebo v prípade, ak spracúva osobné údaje v priamom rozpore s pokynmi prevádzkovateľa.

Zároveň si dovoľujeme stručne načrtnúť niektoré povinnosti prevádzkovateľov resp. sprostredkovateľov v zmysle GDPR, ktoré považujeme za vhodné spomenúť vzhľadom na ich dôležitosť z hľadiska zásady zodpovednosti.

2.2.1 Základné zásady spracúvania osobných údajov z pohľadu zamestnávateľa

Základné zásady spracúvania osobných údajov majú svoju dlhú tradíciu v medzinárodných dokumentoch týkajúcich sa regulácie ochrany osobných údajov. Počas posledných 30 rokov však prešli určitým vývojom, aby sa dostali do súčasnej podoby.[61]

Základné zásady reflektujú základné piliere, na ktorých spracúvanie osobných údajov stojí a padá. Súlad so základnými zásadami je základom pri spracúvaní osobných údajov a z jednotlivých zásad pramenia aj konkrétne inštitúty GDPR. Navyše, základné zásady slúžia ako interpretačné pravidlá, na základe ktorých je nutné vykladať jednotlivé ustanovenia GDPR v prípade konfliktu alebo nejasného výkladu.

Článok 5 GDPR upravuje šesť zásad spracúvania osobných údajov:

a) Zásada zákonnosti podľa článku 5 ods. 1 písm. a) GDPR;

b) Zásada obmedzenia účelu podľa článku 5 ods. 1 písm. b) GDPR;

c) Zásada minimalizácie údajov podľa článku 5 ods. 1 písm. c) GDPR;

d) Zásada správnosti podľa článku 5 ods. 1 písm. d) GDPR;

e) Zásada minimalizácie uchovávania údajov podľa článku 5 ods. 1 písm. e) GDPR;

[61] K tomu pozri MESARČIK, M. Ochrana osobných údajov. In ANDRAŠKO, J. – HORVAT, M. – MESARČÍK, M.: Vybrané kapitoly práva informačných technológií I. Bratislava: Univerzita Komenského v Bratislave, 2019.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

f) Zásada integrity a dôvernosti podľa článku 5 ods. 1 písm. f) GDPR;

g) Zásada zodpovednosti podľa článku 5 ods. 2 GDPR.

2.2.1.1 Zásada zákonnosti (spravodlivosti a transparentnosti)

Článok 5 ods. 1 písm. a) GDPR ustanovuje, že osobné údaje musia byť spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe. Predmetná zásada obsahuje tri atribúty: zákonnosť, spravodlivosť a transparentnosť.

Zákonnosť spracúvania osobných údajov spočíva v dvoch úrovniach. V prvom rade je potrebné osobné údaje spracúvať na jednom alebo viacerých právnych základoch podľa článku 6 GDPR. To znamená, že každý účel vymedzený prevádzkovateľom musí byť previazaný s jedným alebo viacerými právnymi základmi podľa článku 6 GDPR. Predmetný článok upravuje 6 právnych základov:. Z hľadiska vhodnosti využívania v pracovnoprávnych vzťahoch sa právnym základom budeme venovať v osobitnej časti predkladanej analýzy.

Druhá úroveň zásady zákonnosti reflektuje požiadavku, aby spracúvanie osobných údajov bolo ako také v súlade s celým právnym poriadkom.

Ďalším atribútom tejto zásady je spravodlivosť. Spracúvanie osobných údajov musí byť spravodlivé (*fair*) pre dotknuté osoby. V tomto smere je možné zvýrazniť aspekt dôvery medzi prevádzkovateľom a dotknutou osobou.[62]

Posledným atribútom predmetnej zásady je transparentnosť. Táto požiadavka je reflektovaná vo viacerých požiadavkách a inštitútoch GDPR. Azda najvýznamnejšia súčasť zásady transparentnosti je plnenie informačnej povinnosti prevádzkovateľov v zmysle článkov 12, 13 a 14 GDPR. Dotknutá osoba má právo vedieť určité informácie o spracúvaní osobných údajov a prevádzkovatelia sú povinní im tieto informácie proaktívne poskytnúť. Dotknutá osoba tak má napríklad právo vedieť na aké účely sú jej osobné údaje spracúvané, či dochádza k cezhraničnému prenosu do tretej krajiny, ako prevádzkovateľ osobné údaje získava či ako dlho plánuje prevádzkovateľ osobné údaje uchovávať. Článok 13 GDPR upravuje kategórie

[62] Viac k tomu BERTHOTY, J. a kol. : Všeobecné nariadenie o ochrane osobných údajov. C.H. Beck. Praha, 2018, s. 203 – 204.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

informácií poskytnutých v prípade ich získania priamo od dotknutej osoby a naopak, článok 14 GDPR upravuje kategórie informácií poskytnutých v prípade ich získania inak ako od dotknutej osoby napr. prostredníctvom verejnej dostupných registrov.

Článok 12 ods. 1 GDPR navyše ustanovuje spôsobom, akým je nutné dané informácie poskytnúť, konkrétne „v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho, a to najmä v prípade informácií určených osobitne dieťaťu." Informácie je možné poskytnúť v písomnej podobe alebo elektronicky, pričom prevádzkovatelia najčastejšie volia poskytnutie daných informácií v rámci tzv. Podmienok ochrany súkromia zverejnených na svojom webovom sídle.

Zároveň sú súčasťou zásady transparentnosti ďalšie dva inštitúty a to komunikácia práv dotknutej osoby a komunikácia porušení ochrany osobných údajov dotknutým osobám. V prípade ak dôjde ku bezpečnostnému incidentu (napr. hacknutie systému alebo únik údajov), ktorý možno kvalifikovať ako porušenie ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, tak prevádzkovateľ musí dotknutú osobu na to upozorniť.

2.2.1.2 Zásada obmedzenia účelu

Zásada obmedzenia účelu podľa článku 5 ods. 1 písm. b) GDPR znamená, že osobné údaje musia byť získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi. Účelom možno rozumieť cieľ resp. dôvod, s ktorým sa osobné údaje spracúvajú. Na základe účelu je možné určiť požadovanú správnosť osobných údajov, ich potrebnosť, dobu uchovávania a iné kľúčové faktory ovplyvňujúce spracúvanie osobných údajov. Účel musí byť konkrétny, výslovne uvedený a legitímny.[63] Prevádzkovatelia zvyknú vymedzovať účely všeobecnejšie a následne pripojiť charakteristiku, čo ktorý účel znamená.

Druhým prvkom zásady vymedzenia účelu je tzv. test kompatibility (zlúčiteľnosti) nových účelov. Ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo

[63] K tomu pozri Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation, s. 15-16.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

historického výskumu či štatistické účely sa v súlade s článkom 89 ods. 1 GDPR nepovažuje za nezlučiteľné s pôvodnými účelmi. To znamená, že výskumné alebo štatistické účely za splnenia požiadaviek GDPR je možné robiť na základe už získaných dát automaticky.

Nižšie uvádzame typické účely spracúvania, ktorými štandardne disponuje zamestnávateľ voči zamestnancom.

Účel spracúvania	Charakteristika
Personalistika a mzdy	Ide o účel, ktorý pokrýva základné spracúvanie osobných údajov medzi zamestnávateľom a zamestnancom vyplývajúce z pracovnej zmluvy a Zákonníka práce či predpisov na zabezpečenie bezpečnosti a ochrany zdravia pri práci.
Bezpečnosť a ochrana majetku	Ak zamestnávateľ monitoruje určité statky prostredníctvom monitorovacích zariadení, tento účel musí byť pokrytý ako osobitný účel spracúvania osobných údajov.
Monitorovacie mechanizmy zamestnávateľa	Ak zamestnávateľ monitoruje pracovnú disciplínu alebo má iný dôvod pre implementáciu monitorovacieho mechanizmu v zmysle Zákonníka práce, tieto operácie by mal pokrývaš osobitný účel.
Daňové a účtovné účely	Spracúvanie osobných údajov v zmysle povinností podľa právnych predpisov v oblasti daní a účtovníctva.
Zverejňovanie informácií o zamestnancoch	Ak sa zamestnávateľ rozhodne zverejniť akékoľvek osobné údaje zamestnanca napríklad prostredníctvom webového sídla, tento úkon je

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

	nevyhnutné pokryť v osobitnom účele spracúvania.
Zákonné povinnosti zamestnávateľa	Akékoľvek zákonné povinnosti vyplývajúce z osobitných predpisov ako napríklad spracúvanie osobných údajov na účely súladu s požiadavkami pre whistleblowing.

Ak chce prevádzkovateľ využiť osobne údaje na iný účel ako pôvodný, posudzujeme aj test zlučiteľnosti účelov na inú spracovateľskú operáciu ako pôvodne vymedzenú. V prípade ak napr. spoločnosť predávajúca nábytok spracúva údaje o svojich zákazníkoch za účelom efektívnej donášky tovaru k zákazníkovi, nemôže použiť predmetné údaje na marketingové účely v podobe posielania adresných letákov na základe predchádzajúcich nákupov. GDPR ustanovuje 5 faktorov, ktoré by mal prevádzkovateľ zohľadniť pri posúdení, či sú účely zlučiteľné alebo nie.[64]

2.2.1.3 Zásada minimalizácie údajov

Zásada minimalizácie údajov v zmysle článku 5 ods. 1 písm. c) GDPR znamená, že osobné údaje musia byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. Prevádzkovateľ je povinný prihliadať na spracúvanie dostatočne kvalitných (správnych) osobných údajov o dotknutej osobe na naplnenie vymedzeného účelu. Avšak zároveň je povinný nepracovať s viac údajmi ako je na výkon špecifickej spracovateľskej operácie potrebné. Prevádzkovateľ by tak mal vyhodnotiť proporcionalitu a nevyhnutnosť zozbieraných údajov voči určenému účelu. Napríklad univerzita by nemala spracúvať údaj o krvnej skupine svojich študentov, nakoľko tento údaj nie je nevyhnutný na poskytovania štúdia. Iná situácia by bola, ak by univerzita poskytovala študentom stáž v rámci rizikovejších povolaní ako napr. práca v bani.

[64] Pozri článok 6 ods. 4 GDPR.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Španielsky dozorný orgán riešil prípad,[65] v ktorom zamestnávateľ, ktorý bol majiteľom reštaurácie nahrával prostredníctvom kamier a zvukových zariadení svojich zamestnancov na rôznych miestach vo svojej prevádzke ako toalety, prezliekarne či šatne. Zariadenia na vyhotovenie zvukových a obrazových záznamov mal prevádzkovateľ ukryté a po ich objavení bol zamestnancami podaný podnet. Napriek tomu, že prevádzkovateľ informoval svojich zamestnancov, že zábery a nahrávky môže použiť na pracovnoprávne účely, neinformoval svojich zamestnancov o presnej polohe monitorovacích zariadení.

Za takéto konanie španielsky dozorný orgán uložil pokutu 20 000 € a svoje rozhodnutie odôvodnil troma hlavnými závermi. V prvom rade, dozorný orgán uviedol, že nieto pochýb o tom, že nahrávanie videozáznamov a zvukových nahrávok napĺňa definíciu spracúvania a osobných údajov. V druhom rade, predmetné spracúvanie zasahovalo do intímneho priestoru zamestnancov a podľa dozorného orgánu nebolo v súlade so zásadou minimalizácie uchovávania údajov podľa článku 5 ods. 1 písm. c) GDPR. Zároveň, španielske právo v tomto smere vyžadovalo naplnenie princípu proporcionality a minimálneho zásahu pri monitorovaní zamestnancov. Po tretie, prevádzkovateľ nezohľadnil staršie rozhodnutie španielskeho súdu, ktoré nahrávky medzi zamestnancami charakterizovalo ako nie opodstatnené pri pracovnoprávnych povinnostiach. Skryté monitorovanie zamestnancov tak nemalo ani právny základ a porušovalo viaceré ustanovenia GDPR.

2.2.1.4 Zásada správnosti

Zásada správnosti osobných údajov podľa článku 5 ods. 1 písm. d) GDPR znamená, že osobné údaje musia byť správne a podľa potreby aktualizované. Prevádzkovateľ je zároveň povinný prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia. Považujeme za nutné zvýrazniť, že zásada správnosti osobných údajov sa vždy musí posudzovať vzhľadom na účel spracúvania. V prípade, ak je účel spracúvania priam závislý od správnosti údajov, údaje musia byť aktuálne a správne. Napríklad univerzita si musí od študentov pri prijímacom konaní

[65] Dostupné na: https://www.aepd.es/es/documento/ps-00178-2022.pdf.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

overiť, či získali požadované stredoškolské vzdelanie. Nemusí však overovať študentom poskytnuté informácie v životopise o brigáde počas letných mesiacov.

Rozhodnutie maďarského dozorného orgánu v tomto smere poskytuje určité usmernenie.[66] Zamestnanec sa u svojho zamestnávateľa domáhal zmeny adresy trvalého pobytu, pričom svoje žiadosti o zmenu opakovane zasielal prostredníctvom e-mailových správ v rámci firemnej komunikácie. Po skončení pracovného pomeru bývalý zamestnanec upozorňoval na spracúvanie osobných údajov bez jeho súhlasu. Maďarský dozorný orgán prípad preskúmal a v bode týkajúcom sa zmeny adresy trvalého pobytu konštatoval porušenie GDPR pre nesplnenie žiadosti o opravu údajov. Zamestnávateľ tak spracúval nesprávne osobné údaje, mal o tom objektívnu vedomosť a napriek tomu údaje neopravil. Zároveň kritizoval, že zamestnávateľ neodpovedal na žiadosť dotknutej osobe v predpísanej lehote (mesiac) a tým porušil články týkajúce sa transparentnosti a informačnej povinnosti.

2.2.1.5 Zásada minimalizácie uchovávania údajov

Zásada minimalizácie údajov podľa článku 5 ods. 1 písm. e) GDPR reflektuje požiadavku, že osobné údaje sú uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú. Osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely (v súlade s článkom 89 ods. 1 GDPR) za predpokladu prijatia primeraných technických a organizačných opatrení. Údaje, ktoré už nie sú potrebné a uplynie lehota na ich uchovávanie je potrebné zlikvidovať resp. vymazať. Doby uchovávania v niektorých prípadoch určujú aj osobitné právne predpisy. Napríklad Zákonník Práce ustanovuje doby pre uchovávanie spisu zamestnanca. Doba uchovávania môže byť určená číselne alebo slovne (počas trvania zmluvy, pokým neuplynie premlčacia doba a podobne).

2.2.1.6 Zásada integrity a dôvernosti (bezpečnosť)

[66] Dostupné na: https://www.naih.hu/files/NAIH-2020-193-hatarozat.pdf

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Článok 5 ods. 1 písm. f) GDPR upravuje zásadu bezpečnosti a integrity, ktorá znamená, že osobné údaje musia byť spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení. Táto zásada sa nevzťahuje len na vonkajšie hrozby narušenia bezpečnosti (únik údajov spôsobený hackermi alebo krádež počítača), ale aj v rámci vnútornej štruktúry prevádzkovateľa (nedostatočne vyškolených zamestnancov). Bezpečnosť spracovateľských operácií by mala byť predovšetkým zaručená prostredníctvom rôznych technických a organizačných opatrení ako napr. obmedzeným prístupom k údajom (autorizovaním konkrétnych osôb), konkrétnymi povereniami autorizovaných osôb, ktorí môžu pracovať s osobnými údajmi a implementáciou režimu obnovenia dát v prípade omylu alebo straty.

Na bezpečnosť spracúvania osobných údajov nadväzujú predovšetkým dva inštitúty GDPR. V prvom rade ide požiadavku článku 32 GDPR ktorý ustanovuje, že prevádzkovatelia by mali prijať primerané bezpečnostné opatrenia so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb. V druhom rade ide o inštitútu Nahlasovania porušení ochrany osobných údajov v zmysle článkov 33 a 34 GDPR – prevádzkovatelia majú povinnosť nahlasovať bezpečnostné incidenty s charakterom porušenia ochrany osobných údajov dozornému orgánu prípadne dotknutým osobám podľa závažnosti incidentu a vzniknutého rizika.[67]

Porušenia zásady bezpečnosti sú jedny v praxi najčastejších porušení GDPR. Ako príklad možno uviesť mediálne známu situáciu zo Slovenskej republiky, keď sa v blízkosti verejne dostupnej skládky objavilo množstvo dokumentov, ktoré obsahovali osobné údaje. Prevádzkovateľ tak v tomto prípade nedostatočne zabezpečil precízne zničenie osobných údajov.[68]

[67] K tomu pozri článok 33 GDPR a článok 34 GDPR.
[68] Pozri viac https://www.dataprotection.gov.sk/uoou/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Talianske mesto Bolzano dostalo pokutu vy výške 84 000 € z dôvodu všeobecného monitorovania zamestnancov, pričom v rámci svojich aktivít porušilo viacero ustanovení GDPR vrátane pravidiel pre zákonnosť spracúvania či článku 88 GDPR. Sťažovateľ v danom prípade namietal, že jeho zamestnávateľ (mesto Bolzano) porušil pravidlá na ochranu osobných údajov tým, že monitoroval prevádzku internetovej siete a prístupov do siete svojich zamestnancov. Problematické bolo technické nastavenie zberu dát, ktorý v zásade ukladal a monitoroval každú navštívenú stránku, čas prezerania a ďalšie súvisiace údaje. Zároveň, doba uchovávania týchto údajov bola neprimerane dlhá. Zamestnanci o danom spracúvaní údajov neboli vôbec informovaní. Vyšetrovanie dozorného orgánu odhalilo, že daný systém fungoval 10 rokov, údaje o jednotlivých zamestnancoch a ich aktivite na internete uchovával mesiac a zároveň boli z týchto dát vyrábané pravidelné správy na účely detekcie rizík pre informačnú bezpečnosť. Vzhľadom na to, že zamestnanci o danom spracúvaní neboli informovaní a spracúvanie boli neproporcionálne vzhľadom na deklarovaný účel, taliansky dozorný orgán takéto konanie vyhodnotil ako porušenie GDPR. Zvýraznený bol predovšetkým fakt, že monitorovanie zahŕňalo aj spracúvanie údajov, ktoré nemali s pracovnou činnosťou zamestnanca nič spoločné. Taliansky dozorný orgán argumentoval, že potreba znížiť riziko nesprávneho používania surfovania na internete nemôže viesť k úplnému zrušeniu akéhokoľvek očakávania súkromia zo strany zamestnanca na pracovisku, a to ani vtedy, keď zamestnanec využíva sieťové služby sprístupnené zamestnávateľom na súkromné účely. Mesto Bolzano tak po tomto rozhodnutí muselo zmeniť svoje procesy spracúvania údajov z technického a organizačného hľadiska.[69] Monitorovanie bezpečnosti siete patrí u mnohých podnikateľov k bežným aktivitám. Ako ukazuje rozhodnutie talianskeho dozorného orgánu vyššie, bezpečnosť nemôže ísť nikdy na úkor ochrany súkromia zamestnancov. Dané monitorovanie siete síce trpelo viacerými neduhmi (doba uchovávania, transparentnosť), avšak základná výstraha je jasná: proporcionalita musí byť zachovaná a bezbrehé monitorovania navštevovaných stránok zamestnancov nemusí daný princíp spĺňať.

2.2.1.7 Zásada zodpovednosti

[69] Garante per la protezione dei dati personali (Italy) – 9669974. Dostupné na: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9669974.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Zásada zodpovednosti je v GDPR koncipovaná veľmi stručne, napriek tomu v sebe subsumuje niekoľko povinností, na ktoré poukážeme. Podľa článku 5 ods. 2 je prevádzkovateľ zodpovedný za súlad s vyššie uvedenými zásadami a musí vedieť tento súlad preukázať. Na základe usmernenia Pracovnej skupiny čl. 29[70] zásadu zodpovednosti tvorí (i) aktívna a preventívna činnosť prevádzkovateľov (zavedenie opatrení, ktoré zaručia dodržiavanie pravidiel a politík ochrany osobných údajov) a dokumentárna/záznamová činnosť prevádzkovateľov (príprava dokumentov, ktoré preukazujú súlad s pravidlami ochrany osobných údajov).

GDPR reflektuje zásadu zodpovednosti vo viacerých inštitútoch ako posúdenie vplyvu, špecificky navrhnutá a štandardná ochrana osobných údajov, vedenie záznamov o spracovateľských operáciách či určenie zodpovednej osoby. Vedenie záznamov o spracovateľských operáciách v zmysle článku 30 GDPR je ďalšou povinnosťou, v zmysle ktorej prevádzkovatelia a sprostredkovatelia sú povinní viesť dokumenty, v ktorých detailne mapujú na aké účely osobné údaje spracúvajú, o akých osobách, kto k nim má prístup atď. Tieto záznamy by mali slúžiť ako podklad, ktorý mapuje spracúvanie osobných údajoch v danej organizácií.[71]

2.2.2 Posúdenie vplyvu na ochranu údajov a pracovnoprávne vzťahy

Posúdenie vplyvu na ochranu údajov (*Data protection impact assessment – DPIA*) je novým inštitútom pri spracúvaní osobných údajov, ktorý substituuje viaceré notifikačné povinnosti. DPIA je pevnou súčasťou zásady zodpovednosti, ktorá reflektuje preventívne povinnosti pre prevádzkovateľov predchádzať a zmierňovať neželané riziká pri spracúvaní osobných údajov. Podstatou daného inštitútu je analýza právnych rizík pri spracúvaní osobných údajov a vypracovanie dokumentu, ktorý danú povinnosť dokumentuje. Toto posúdenie sa musí vykonať pred[72] samotným začatím spracúvania osobných údajov. Tento inštitút je obzvlášť dôležitý v kontexte využívania nových technológií pri spracúvaní osobných údajov. Výbor vydal usmernenie k posúdeniu vplyvu na ochranu údajov, ktoré daný proces vysvetľuje a precizuje.[73]

[70] Article 29 Data Protection Working Party Opinion 03/2010 on the principle of accountability, s. 9.
[71] Pozri viac článok 30 GDPR.
[72] Pozri článok 35 ods. 1 GDPR.
[73] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation, 2016/679.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Povinnosť vykonať posúdenie vplyvu na ochranu údajov je viazaná na špecifické podmienky, ktoré sú upravené v článkoch 35 ods. 3 (špecifické prípady) a 35 ods. 1 (všeobecná klauzula) GDPR. Prevádzkovateľ by mal v praxi najprv posúdiť, či sa naňho nevzťahuje jeden zo špecifických prípadov uvedených v článku 35 ods. 3 GDPR a ak nie, analyzovať podmienky všeobecnej klauzuly v článku 35 ods. 1 GDPR. Na tomto mieste je taktiež nutné doplniť, že v zmysle článku 35 ods. 4 GDPR bol každý dozorný orgán členského štátu povinný vypracovať a zverejniť zoznam tých spracovateľských operácií, ktoré podliehajú požiadavke na posúdenie vplyvu na ochranu údajov. Úrad na ochranu osobných údajov Slovenskej republiky takýto zoznam taktiež publikoval.[74]

Článok 35 ods. 3 GDPR ustanovuje, že posúdenie vplyvu sa vykoná najmä v prípadoch:

- systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu;
- spracúvania vo veľkom rozsahu osobitných kategórií údajov podľa článku 9 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10, alebo;
- systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

Diskutovaný článok obsahuje demonštratívny výpočet prípadov, keď prevádzkovateľ bude mať povinnosť posúdenie vplyvu vykonať. Ako je evidentné z tohto výpočtu, dané prípady obsahujú veľké množstvo právne neurčitých pojmov ako systematické a rozsiahle hodnotenie, veľký rozsah alebo verejne prístupné miesto. Tieto termíny bližšie charakterizuje usmernenie Výboru.

[74] Pozri Úrad na ochranu osobných údajov SR: Zoznam spracovateľských operácií podliehajúcich posúdeniu vplyvu na ochranu osobných údajov Slovenskej republiky. Dostupné na https://dataprotection.gov.sk/uoou/sites/default/files/zoznam_spracovatelskych_operacii_ktore_podliehaju_posudeniu_vplyvu.pdf.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Ak prevádzkovateľ nenašiel posudzovanú spracovateľskú operáciu v špecifickej klauzule článku 35 ods. 3 GDPR, automaticky to neznamená že DPIA nemá vykonať. Povinnosť vykonať DPIA totiž môže vyplynúť aj po analýze kritérií v kontexte všeobecnej klauzuly podľa článku 35 ods. 1 GDPR. Článok 35 ods. 1 GDPR ustanovuje, že *„...ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, môže byť dostatočné jedno posúdenie."*[75] Rozhodujúcim faktorom pre vykonanie posúdenia vplyvu je tak miera rizika pre práva a slobody fyzických osôb (vyžaduje sa vysoké riziko).

Na účely posúdenia vplyvu definoval Výbor niekoľko kritérií, ktoré by mal prevádzkovateľ vziať do úvahy pri posúdení miery rizika spracúvania osobných údajov. Na aktiváciu všeobecnej klauzuly posúdenia vplyvu stačí, ak sú splnené dve nižšie uvedené kritériá, ktoré uvádzame v tabuľke s krátkou charakteristikou:

Kritérium	Charakteristika
Vyhodnocovanie určitých aspektov týkajúcich sa dotknutej osoby	Výbor vo svojom usmernení výslovne zahŕňa medzi príklady vyhodnocovania určitých aspektov dotknutých osôb profilovanie a vytváranie predpovedí o dotknutej osobe. Medzi relevantnými aspektmi demonštratívne uvádza hodnotenie činnosti dotknutej osoby v rámci výkonu práce, jej majetkových pomerov, zdravia, osobných preferencií alebo záujmov, spoľahlivosti alebo správania, polohy alebo pohybu.

[75] GDPR, článok 35 ods. 1.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Automatizované rozhodovanie s právnym alebo podobne závažným účinkom	Druhým indikátorom je, že spracúvanie osobných údajov je vykonané automatizovane s automatizovaným rozhodnutím, ktoré má právny alebo podobne závažný účinok na dotknutú osobu. Zjednodušene povedané, automatizované rozhodovanie je taký proces, v ktorom nie je prítomný ľudský zásah.
Systematické monitorovanie osobných údajov	Systematické monitorovanie údajov je potrebné interpretovať v intenciách takých situácií, keď sú dotknuté osoby pozorované, kontrolované a monitorované vrátane sledovania prostredníctvom internetovej siete. Je prakticky nemožné nebyť predmetom takéhoto monitorovania. Monitorovanie verejne dostupných miest zahŕňa napríklad verejné priestranstvá, knižnice, úrady alebo obchodné domy.
Spracúvanie citlivých osobných údajov	Ďalším indikátorom je spracúvanie citlivých osobných údajov a údajov týkajúcich sa páchania priestupkov a trestných činov. Navyše Výbor uvádza, že medzi citlivé osobné údaje možno zahrnúť aj osobné dokumenty, elektronické správy, denníky, poznámky a údaje spracúvané v rámci mobilných aplikácií, ktoré odhaľujú osobnostné aspekty o dotknutých osobách.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Spracúvanie údajov vo veľkom rozsahu	Posúdenie vplyvu na ochranu údajov je potrebné vykonať aj v prípadoch, ak sa spracúvanie vykonáva vo veľkom rozsahu. Výbor menuje faktory, ktoré indikujú, či ide o spracúvanie osobných údajov vo veľkom rozsahu alebo nie – (i) počet dotknutých osôb, (ii) kvantita údajov a ich rozsah, (iii) doba spracovateľskej operácie a (iv) geografický rozsah spracúvania osobných údajov.
Spájanie alebo kombinovanie súborov a údajov pochádzajúcich z rôznych spracovateľských operácií	Ďalším indikátorom je spájanie a kombinovanie údajov z rôznych zdrojov alebo od rôznych prevádzkovateľov.
Spracúvanie údajov týkajúcich sa *„zraniteľných“* dotknutých osôb	Zraniteľné osoby sú v diskutovanom usmernení Výbor vymedzené ako také osoby, ktoré nie sú v rovnoprávnom postavení voči prevádzkovateľovi. Ako príklad možno opätovne uviesť občanov voči orgánom verejnej moci alebo zamestnanca voči zamestnávateľovi.
Využitie nových technológií, technologických alebo organizačných riešení a postupov	Ako nové technológie Výbor uvádza ako príklad *blockchain*, algoritmy na báze umelej inteligencie alebo internet vecí.
Spracúvanie bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu	Ku spracúvaniu údajov, ktoré bráni dotknutým osobám uplatniť svoje právo alebo využiť službu alebo zmluvu, dochádza napr. vtedy, keď banka preverí klienta v

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

	referenčnej databáze úverov a na základe toho s ním neuzavrie zmluvu.

Pri vzťahoch zamestnávateľ a zamestnanec budú typické prípady, kedy zamestnávateľ bude musieť vypracovať posúdenie vplyvu na ochranu údajov zahŕňať najmä:

- Monitorovanie kamerovými systémami
- Monitorovanie vozidiel
- Zabezpečenie vstupu do priestorov prostredníctvom špecifických autentifikačných mechanizmov
- Automatizované vyhodnocovanie výkonnosti zamestnancov.

Metodologický základ, ako posúdenie vplyvu efektívne urobiť, poskytuje samotné GDPR a vyhláška Úradu na ochranu osobných údajov Slovenskej republiky z 29. mája 2018 o postupe pri posudzovaní vplyvu na ochranu osobných údajov. GDPR v článku 35 ods. 7 upravuje, že posúdenie vplyvu by malo najmä obsahovať tieto všeobecné body:

- systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ
- posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu
- posúdenie rizika pre práva a slobody dotknutých osôb uvedeného v odseku 1 a
- opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením, pričom sa zohľadnia práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka.

2.2.3 Súhlas a iné právne základy spracúvania osobných údajov v kontexte pracovnoprávnych vzťahov

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Zásada zákonnosti ustanovuje, že osobné údaje musia byť spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe. Čo konkrétne znamená pojem *„zákonne“*, explicitne ustanovuje článok 6 GDPR, ktorý za zákonné spracúvanie osobných údajov považuje iba takú spracovateľskú operáciu, pri ktorej prevádzkovateľ disponuje platným právnym základom. Ku každému účelu spracúvania osobných údajov musí existovať vhodný právny základ, pričom ich môže byť aj viac. Právny základ možno charakterizovať ako právny dôvod na spracúvanie osobných údajov. Najčastejšie sa vyskytujúcim právnym základom je osobitný zákon, ktorý ustanovuje konkrétnym prevádzkovateľom povinnosť spracúvať osobné údaje. Neplatí, že súhlas je privilegovaným právnym základom a nemá ani osobitné postavenie medzi ostatnými právnymi základmi. GDPR upravuje šesť právnych základov:

- súhlas[76]
- plnenie zmluvy[77]
- zákonnú povinnosť[78]
- ochranu životne dôležitých záujmov dotknutej alebo inej fyzickej osoby[79]
- verejný záujem[80]
- oprávnený záujem prevádzkovateľa (legitímny záujem).[81]

[76] Článok 6 ods. 1 písm. a) GDPR: „dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely.“
[77] Článok 6 ods. 1 písm. b) GDPR: „spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy.“
[78] Článok 6 ods. 1 písm. c) GDPR: „spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa.“
[79] Článok 6 ods. 1 písm. d) GDPR: „spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby.“
[80] Článok 6 ods. 1 písm. e) GDPR: „spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.“
[81] Článok 6 ods. 1 písm. f) GDPR: „spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobou dieťa.“

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Pri vymedzení právneho základu je potrebné podľa nášho názoru postupovať nasledovným spôsobom: V prvom rade je vhodné posúdiť, či spracúvanie osobných údajov nie je nevyhnutné na plnenie zmluvy alebo či nejde o zákonnú povinnosť, prípadne úlohu vo verejnom záujme. Následne je vhodné upriamiť pozornosť na právny základ oprávneného záujmu a jeho použiteľnosť. Ak sme vylúčili všetky predchádzajúce možnosti, do úvahy prichádza len životne dôležitý záujem (ktorý sa však v praxi používa minimálne a iba vo veľmi špecifických situáciách), prípadne súhlas, ktorý je „poslednou záchranou." Totožný postup platí všeobecne pre prevádzkovateľov a taktiež pre zamestnávateľov v pozícii prevádzkovateľa.

2.2.3.1 Súhlas

Súhlas je jedným z „najkrehkejších" právnych základov a jediným, ktorým môže plne disponovať dotknutá osoba. To prakticky znamená, že ak dotknutá osoba svoj súhlas odvolá (na čo má v zmysle GDPR právo), prevádzkovateľ je povinný prestať spracúvať osobné údaje na daný súhlas. Nižšie analyzujeme definičné znaky súhlasu a osobitne aspekty a podmienky jeho vyjadrenia.

Súhlas je definovaný v článku 4 bode 11 GDPR ako „akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka". EDPB k danej definícii vydal osobitné usmernenie,[82] ktoré vymenúva 5 kritérií danej definície, a to:

- prejavenie súhlasu
- sloboda
- konkrétnosť
- informovanosť a
- jednoznačnosť.

[82] European Data Protection Board. Guidelines on Consent under Regulation 2016/679.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Prvým kritériom je **prejav** súhlasu. Tento prejav môže byť urobený viacerými spôsobmi, ako napr. podpisom, ústnou deklaráciou, zaškrtnutím políčka, kliknutím na políčko alebo akoukoľvek aktivitou dotknutej osoby za splnenia ďalších kritérií.

Druhým kritériom je, že súhlas musí byť daný **slobodným** spôsobom. To prakticky znamená, že dotknutá osoba má dostatok slobodnej vôle pri rozhodovaní, či súhlas udelí alebo neudelí a nie je pri tomto rozhodovaní vystavovaná tlaku. GDPR vo svojom texte výslovne spomína tri situácie, keď je sloboda udelenia súhlasu kompromitovaná.

Prvú situáciu predstavuje jednoznačný nepomer v postavení medzi prevádzkovateľom a dotknutou osobou. GDPR uvádza ako príklad spracúvanie osobných údajov občanov orgánmi verejnej moci.[83] Toto konštatovanie však neplatí absolútne a v praxi sa môžu vyskytovať situácie, keď orgány verejnej moci môžu súhlas ako právny základ použiť bez indikácie nedostatku slobodnej vôle dotknutej osoby (napr. pri súhlase so zverejňovaním fotografií.[84] Ďalším príkladom jednoznačného nepomeru v postavení je vzťah zamestnanec – zamestnávateľ, kde je zamestnanec slabšou stranou a neudelenie súhlasu môže mať nepriaznivé dôsledky z hľadiska jeho pracovného zaradenia alebo iných aspektov.[85]

Druhou situáciou kompromitovania slobody udelenia súhlasu je, „ak nie je možné dať samostatný súhlas na jednotlivé spracovateľské operácie osobných údajov napriek tomu, že by to bolo v konkrétnom prípade vhodné[86]“. Ak je to možné, dotknutá osoba by mala mať jednoduchým spôsobom možnosť udeliť súhlas na jednotlivé spracovateľské operácie.

Treťou situáciou kompromitovania slobody udelenia súhlasu je podmieňovanie použitia služby udeleným súhlasu (tzv. *bundling*). Tento problém reflektuje článok 7 ods. 4 GDPR: *„pri posudzovaní, či bol súhlas poskytnutý slobodne, sa v čo najväčšej miere okrem iného zohľadní skutočnosť, či sa plnenie zmluvy vrátane poskytnutia služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný“.* To znamená, že ak na poskytnutie služby je vyžadovaný súhlas so spracúvaním osobných údajov a tento

[83] Pozri Recitál 43 GDPR.
[84] Pozri European Data Protection Board. Guidelines on Consent under Regulation 2016/679, s. 6 – 7.
[85] Tamže.
[86] Recitál 43 GDPR.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

súhlas nie je z objektívnych príčin nevyhnutný, išlo by o porušenie daného článku a súhlas by nebol považovaný za daný slobodne[87].

Tretím kritériom je, že súhlas musí byť poskytnutý **konkrétne**. Konkrétnosť spočíva v troch aspektoch, a to: (i) poskytnutie súhlasu na konkrétne vopred vymedzené účely spracúvania osobných údajov; (ii) možnosť poskytnutia súhlasu na viaceré spracovateľské operácie a účely jednotlivo, ak je to možné a vhodné a; (iii) oddelenie informácií o spracúvaní osobných údajov na základe súhlasu od iných informácií (napr. všeobecných zmluvných podmienok alebo iných právnych dojednaní).

Štvrtým kritériom je **informovanosť** súhlasu. Informovaný súhlas je taký súhlas, pri ktorého poskytovaní majú dotknuté osoby dostatok informácií o spracúvaní osobných údajov. Tieto požiadavky reflektujú články 12 až 14 GDPR. EDPB odporúča pri poskytovaní súhlasu prevádzkovateľom uvádzať informácie minimálne o

- identite prevádzkovateľa
- účele spracúvania, na ktorý je súhlas vyžadovaný
- type údajov, ktoré sa od dotknutej osoby vyžadujú
- práve dotknutej osoby súhlas odvolať
- či ide o automatizované individuálne rozhodovanie v zmysle článku 22 GDPR
- rizikách spojených s prenosom údajov do tretích krajín[88].

Čo sa spôsobu poskytnutia informácií týka, platia závery týkajúce sa všeobecnej informačnej povinnosti v zmysle článku 12 GDPR[89].

[87] K tomu pozri viac BERTHOTY. J. a kol. Všeobecné nariadenie na ochranu osobných údajov. 1. vydanie. Praha : C. H. Beck, 2018, s. 235 a nasl.
[88] European Data Protection Board. Guidelines on Consent under Regulation 2016/679, s. 13.
[89] Článok 12 ods. 1 GDPR: „Prevádzkovateľ prijme vhodné opatrenia s cieľom poskytnúť dotknutej osobe všetky informácie uvedené v článkoch 13 a 14 a všetky oznámenia podľa článkov 15 až 22 a článku 34, ktoré sa týkajú spracúvania, a to **v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho, a to najmä v prípade informácií určených osobitne dieťaťu. Informácie sa poskytujú písomne alebo inými prostriedkami, vrátane v prípade potreby elektronickými prostriedkami**. Ak o to požiadala

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Piatym kritériom platného súhlasu v zmysle GDPR je jeho **jednoznačnosť** pri prejave vôle. To znamená, že musí ísť o jednoznačne aktívny a pozitívny prejav vôle dotknutej osoby, z ktorej možno jednoznačne vyčítať poskytnutie súhlasu. Túto požiadavku napríklad nespĺňa predvyplnené alebo predzakliknuté okienko pri elektronickom súhlase. Podobné konštatovanie platí pre konkludentný súhlas[90]. Rovnako je súhlas nejednoznačný, ak sa spája so súhlasom s inými právnymi dojednaniami, ako sú napríklad všeobecné obchodné podmienky.

Podmienky vyjadrenia súhlasu upravuje článok 7 GDPR. Ten okrem už analyzovaného ustanovenia článku 7 ods. 4 GDPR (*bundling)* vyžaduje, aby:

- prevádzkovateľ vedel preukázať poskytnutie súhlasu[91]
- žiadosť o poskytnutie súhlasu bola odlíšiteľná od iných právnych dojednaní alebo zmlúv a zároveň táto žiadosť musí byť v zrozumiteľnej a ľahko dostupnej forme a formulovaná jasne a jednoducho[92]
- dotknutá osoba bola informovaná, že má právo svoj súhlas kedykoľvek odvolať a o tejto skutočnosti ju prevádzkovateľ musí informovať pred poskytnutím samotného súhlasu[93].

Využitie súhlasu sa výslovne v pracovnoprávnych vzťahoch nevylučuje, **musí byť ale zabezpečená možnosť zo strany zamestnanca udelenie súhlasu odmietnuť bez negatívnych dôsledkov**. Literatúra ako príklady využitia súhlasu uvádza spracúvanie údajov na účely organizovania aktivít s rodinami a deťmi zamestnancov, zabezpečenie darčekov pre zamestnancov alebo marketingové ponuky určené výslovne pre zamestnancov spoločnosti.[94] Navyše, Úrad na ochranu osobných údajov SR vo svojom usmernení v niektorých prípadoch

dotknutá osoba, informácie sa môžu poskytnúť ústne za predpokladu, že sa preukázala totožnosť dotknutej osoby iným spôsobom."

[90] Recitál 32 GDPR: „Mlčanie, vopred označené políčka alebo nečinnosť by sa preto nemali pokladať za súhlas."

[91] Článok 7 ods. 1 GDPR.

[92] Článok 7 ods. 2 GDPR.

[93] Článok 7 ods. 3 GDPR.

[94] HUDECOVÁ, I. – CYPRICHOVÁ, A. – MAKATURA, I. a kol.: Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár. Eurokódex, 2018, s. 589.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

napriek nerovnováhe subjektov uprednostňuje využitie súhlasu ako právneho základu.[95] Ako uvádza, Pracovná skupina čl. 29 vo svojom usmernení, za platný súhlas v pracovnoprávnych vzťahoch nemožno považovať, ak zamestnanec využíva zariadenie, ktoré má prednastavené zasielanie údajov zamestnávateľovi.[96]

2.2.3.2 Plnenie zmluvy

Druhým právnym základom je plnenie zmluvy. Tento právny základ možno využiť v situáciách, ak je spracúvanie osobných údajov nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy. Predmetný právny základ sa vzťahuje aj na tzv. predzmluvné vzťahy, čiže na spracúvanie osobných údajov vo fáze uzavretia zmluvy, v ktorej je prítomný úprimný úmysel strán danú zmluvu uzatvoriť. Zároveň je tento právny základ pomerne široko využívaný v prípade používania elektronických online služieb, napr. mobilných aplikácií alebo sociálnych sietí.

Na použitie tohto právneho základu je tak absolútne nevyhnutné identifikovať cieľ zmluvy a spracúvanie osobných údajov vrátane jeho rozsahu prispôsobiť danému cieľu. Interpretácia cieľa zmluvy by mala byť pomerne striktná a reštriktívna a prevádzkovateľ by mal naozaj precízne minimalizovať rozsah spracúvania osobných údajov na účely danej zmluvy. EDPB vyžaduje objektívne posúdenie nevyhnutnosti a v kontexte tohto právneho základu a jeho použiteľnosti by si prevádzkovateľ okrem iného mal analyzovať nasledovné atribúty:

- aká je povaha zmluvy a čo je na základe nej poskytnuté dotknutej osobe
- čo je dôvodom na uzavretie danej zmluvy
- aké sú obligatórne znaky danej zmluvy a čo obsahujú

[95] Úrad na ochranu osobných údajov SR: Často kladené otázky k fotografiám a audiovizuálnym záznamom. Dostupné na: https://dataprotection.gov.sk/uoou/sites/default/files/faq_k_fotografiam_a_audio_zaznamom.pdf.
[96] ARTICLE 29 DATA PROTECTION WORKING PARTY: Opinion 2/2017 on data processing at work, 17/EN WP 249, s. 7.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- aké sú očakávania prevádzkovateľa a aké sú očakávania dotknutej osoby pri plnení zmluvy.[97]

Tento právny základ je vysoko relevantný práve v kontexte pracovnoprávnych vzťahov a predzmluvných vzťahov. Jeho využívanie potvrdzuje aj Pracovná skupina čl. 29.[98]

2.2.3.3 Zákonná povinnosť

Zákonná povinnosť je najčastejšie používaný právny základ v praxi, nakoľko množstvo právnych predpisov upravuje spracúvanie osobných údajov v rôznych situáciách u rôznych osôb.

V tomto smere však dodávame, že slovenský preklad Nariadenia nie je celkom správny a nejde iba o povinnosť vymedzenú v zákone, ale o akýkoľvek normatívny právny akt (v anglickom znení *legal obligation*[99]).

V praxi často dochádza k neistote, kedy majú prevádzkovatelia používať právny základ zákonnej povinnosti podľa článku 6 ods. 1 písm. c) GDPR a kedy právny základ verejného záujmu podľa článku 6 ods. 1 písm. e) GDPR. V zmysle metodického usmernenia Úradu na ochranu osobných údajov SR je potrebné rozlišovať príkazové formulácie znení právnej úpravy a prípady, keď ide o možnosť spracúvania osobných údajov[100]. Ak ide o príkazovú formuláciu (napr. prevádzkovateľ je povinný spracúvať..., prevádzkovateľ spracúva tieto údaje..., register obsahuje...), prevádzkovateľ by mal použiť právny základ plnenia zákonnej povinnosti v zmysle článku 6 ods. 1 písm. c) GDPR. Ak ustanovenie obsahuje inú formuláciu ako príkaz (napr. prevádzkovateľ je oprávnený spracúvať osobné údaje o..., prevádzkovateľ môže na tento účel spracúvať osobné údaje..., prípadne akékoľvek iné formulácie odlišné od príkazu), je vhodné použiť právny základ úlohy vo verejnom záujme podľa článku 6 ods. 1 písm. e). Nakoľko na

[97] European Data Protection Board. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.
[98] ARTICLE 29 DATA PROTECTION WORKING PARTY: Opinion 2/2017 on data processing at work, 17/EN WP 249, s. 7.
[99] K tomu pozri HUDECOVÁ, I. – CYPRICHOVÁ, A. – MAKATURA, I. a kol.: *Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár*. Eurokódex, 2018, s. 153 – 154.
[100] Úrad na ochranu osobných údajov SR: Zákonnosť spracúvania osobných údajov. Dostupné na https://dataprotection.gov.sk/uoou/sites/default/files/zakonnost_aktualizovana_verzia_22.01.2019.pdf, s. 5 – 6.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

jeden účel môže byť naviazaných aj viacero právnych základov, nie je možné vylúčiť situácie, keď pri právnej neistote prevádzkovateľa bude vhodné uviesť oba právne základy.

Plnenie zákonných povinností je taktiež častý právny základ v pracovnoprávnych vzťahoch.[101] V slovenskom kontexte možno uviesť spracúvanie osobných údajov na základe Zákonníka práce alebo zákona o BOZP.

2.2.3.4 Životne dôležitý záujem

Ďalším právnym základom je prípad, ak spracúvanie osobných údajov je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby. Tento právny základ je v praxi používaný veľmi ojedinele a bude predovšetkým aplikovateľný na situácie, keď pôjde o záchranu života a zdravia. Tento právny základ dopĺňa Recitál 46 GDPR: *„Spracúvanie osobných údajov by sa malo rovnako považovať za zákonné, ak je potrebné na účely ochrany záujmu, ktorý je zásadný pre život dotknutej alebo inej fyzickej osoby. Spracúvanie osobných údajov na základe životne dôležitom záujme inej fyzickej osoby by sa malo uskutočniť v zásade len vtedy, keď sa takéto spracúvanie zjavne nemôže zakladať na inom právnom základe. Niektoré typy spracúvania môžu slúžiť na dôležité účely verejného záujmu aj životne dôležité záujmy dotknutej osoby, napríklad ak je spracúvanie nevyhnutné na humanitárne účely vrátane monitorovania epidémií a ich šírenia alebo v humanitárnych núdzových situáciách, najmä v prípade prírodných katastrof a katastrof spôsobených ľudskou činnosťou.“*

2.2.3.5 Verejný záujem

Právny základ verejného záujmu upravuje dve odlišné situácie. V prvej situácii ide o spracúvanie osobných údajov nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme. V druhom prípade ide o spracúvanie osobných údajov nevyhnutné pri výkone verejnej moci zverenej prevádzkovateľovi. Vzhľadom na to, že osobám súkromného práva je verejná moc zverená zriedka, druhá časť pôsobnosti tohto právneho základu sa aplikuje na orgány

[101] ARTICLE 29 DATA PROTECTION WORKING PARTY: Opinion 2/2017 on data processing at work, 17/EN WP 249, s. 7.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

verejnej moci[102]. Tento právny základ je použiteľný tak pre orgány verejnej moci, ako aj pre súkromnoprávne osoby. Jedinou požiadavkou v zmysle GDPR pre aplikovanie tohto právneho základu je, že musí vyplývať z osobitného predpisu v národnom právnom poriadku, resp. práve EÚ. Inými slovami, musí existovať právny akt, ktorý ustanoví minimálne možnosť spracúvania osobných údajov na daný účel.

2.2.3.6 Oprávnený záujem

Právny základ oprávneného záujmu predpokladá vypracovanie tzv. balančného testu (*balancing test).*[103] Cieľom tohto balančného testu je preukázať, že oprávnené záujmy prevádzkovateľa prevažujú nad právami, záujmami a slobodami dotknutej osoby. Tento právny základ nie je použiteľný pre orgány verejnej moci pri plnení ich úloh. Interpretáciou tohto právneho základu sa zaoberá WP29 vo svojom staršom stanovisku k oprávnenému záujmu[104]. Niektoré časti predmetného stanoviska sú však už podľa nášho názoru prekonané aj vzhľadom na vývoj judikatúry Súdneho dvora Európskej únie. Konkrétne ide o konkrétne aspekty vykonania balančného testu.

SDEÚ vo veci *Rīgas satiksme*[105] uviedol tri kroky pre vypracovanie balančného testu. V bode 28 daného rozhodnutia predmetný súd judikoval, že na splnenie zákonných požiadaviek oprávneného záujmu musia byť splnené *„tri kumulatívne podmienky, a to po prvé sledovanie legitímneho záujmu osobou zodpovednou za spracovanie alebo tretími osobami, ktorým sú*

[102] K výnimkám z tejto zásady pozri VRABKO, M. a kol. Správne právo hmotné. Všeobecná časť. 1. vydanie. Praha : C. H. Beck, 2012, s. 12 – 13.

[103] Recitál 47 GDPR: „Oprávnené záujmy prevádzkovateľa vrátane prevádzkovateľa, ktorému môžu byť tieto osobné údaje poskytnuté, alebo tretej strany môžu poskytnúť právny základ pre spracúvanie, ak nad nimi neprevažujú záujmy alebo základné práva a slobody dotknutej osoby, pričom sa zohľadnia primerané očakávania dotknutých osôb na základe ich vzťahu k prevádzkovateľovi. Takýto oprávnený záujem by mohol existovať napríklad vtedy, keby medzi dotknutou osobou a prevádzkovateľom existoval relevantný a primeraný vzťah, napríklad keby bola dotknutá osoba voči prevádzkovateľovi v postavení klienta alebo v jeho službách. Existencia oprávneného záujmu by si v každom prípade vyžadovala dôkladné posúdenie vrátane posúdenia toho, či dotknutá osoba môže v danom čase a kontexte získavania osobných údajov primerane očakávať, že sa spracúvanie na tento účel môže uskutočniť. Záujmy a základné práva dotknutej osoby by mohli prevážiť nad záujmami prevádzkovateľa údajov najmä vtedy, ak sa osobné údaje spracúvajú za okolností, keď dotknuté osoby primerane neočakávajú ďalšie spracúvanie.“

[104] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC Adopted on 9 April 2014.

[105] C-13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme.“

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

údaje oznámené, po druhé nevyhnutnosť spracovania osobných údajov na realizáciu sledovaného legitímneho záujmu a po tretie podmienku, že neprevažujú základné práva a slobody osoby, ktorej sa ochrana údajov týka". Tento test v zásade kopíruje požiadavky testu proporcionality pri kolízii dvoch alebo viacerých základných práv a slobôd[106]. V tomto kontexte však proti sebe stojí právo na ochranu osobných údajov dotknutej osoby, jeho záujmy, slobody a oprávnené záujmy prevádzkovateľa.

Prvým krokom balančného testu je **analýza sledovaného oprávneného záujmu**. V zmysle Stanoviska k oprávnenému záujmu tento oprávnený záujem môže vyplývať z výkonu základných práv a slobôd, verejného záujmu (záujmu širšej komunity), prípadne iného oprávneného záujmu (napr. bezpečnosť, ochrana majetku, marketing a pod).[107] Pri determinovaní oprávneného záujmu bude vždy záležať od konkrétneho účelu spracúvania osobných údajov. V rámci prvého kroku považujeme za vhodné, aby v tejto časti balančného testu prevádzkovateľ uviedol, z akého zdroja oprávnený záujem pochádza, či je explicitne dovolený právnym poriadkom, prípadne či nie je právnym poriadkom zakázaný. Zároveň by mal vyhodnotiť aj vplyv oprávneného záujmu na tretie strany (mimo prevádzkovateľa a dotknutej osoby). Pri identifikácii oprávneného záujmu by nemal absentovať ani popis, o aké spracovateľské operácie pôjde, aké typy osobných údajov sa spracúvajú, prípadne aké sú kategórie dotknutých osôb.

Druhým krokom balančného testu je **posúdenie nevyhnutnosti oprávneného záujmu**. Nevyhnutnosť je potrebné odlišovať od proporcionality. Účelom testu nevyhnutnosti je v zmysle dokumentu Európskeho dozorného úradníka pre ochranu údajov posúdenie

[106] Porovnaj napr. I. ÚS 144/2017, bod 3: „Proporcionalita zásahu do základného práva sťažovateľky musí byť odvodená z nevyhnutnej potreby takéhoto zásahu v demokratickej spoločnosti. Test proporcionality je klasicky založený na nasledujúcich troch krokoch. Prvým krokom (A) je test dostatočne dôležitého cieľa (test of legitimate aim/effect), teda test vhodnosti (Geeignetheit) – či zásah smeruje k cieľu, ktorý je dostatočne dôležitý na ospravedlnenie zásahu; a test racionálnej väzby medzi zásahom a cieľom zásahu – či daným prostriedkom (obmedzením slobody prejavu) je možné dosiahnuť akceptovateľný cieľ (ochranu mravnosti). Druhým krokom (B) je test nevyhnutnosti (test potrebnosti použitia daného prostriedku – zásahu (Erforderlichkeit, test of necessity, test of subsidiarity) – teda či nebolo možné použiť šetrnejší zásah. Napokon tretím krokom (C) je test proporcionality v užšom slova zmysle (Angemessenheit, test of proporcionality in the strict sense, proporcionate effect), ktorý zahŕňa jednak (C1) praktickú konkordanciu (praktickú súladnosť), t. j. test zachovania maxima z obidvoch základných práv, a jednak (C2) tzv. Alexyho vážiacu formulu, vážiaci vzorec...".

[107] Tamže, s. 34 a nasl.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

efektívnosti prostriedkov voči deklarovanému cieľu.[108] Pri teste nevyhnutnosti je potrebné dbať na zodpovedanie otázky, či daný účel je možné dosiahnuť aj bez spracúvania osobných údajov a diskusií, či existujú menej invazívne alternatívy dosiahnutia daného účelu.[109] Ak by sme chceli analogicky použiť test nevyhnutnosti ako pri teste proporcionality vyvažovania práv Ústavným súdom SR, tak by mal obsahovať nasledovné:

- zdôvodnenie existencie oprávneného záujmu
- ako spracúvanie osobných údajov dosahuje oprávnený záujem
- či je oprávnený záujem kritický pre fungovanie prevádzkovateľa
- či je oprávnený záujem dôležitý pre fungovanie spoločnosti ako celku
- či je možné dosiahnuť oprávnený záujem bez spracúvania osobných údajov
- aké existujú alternatívy pri dosahovaní oprávneného záujmu
- prečo je spracúvanie osobných údajov vhodnejšie ako iné alternatívy.[110]

Tento výpočet je iba demonštratívny a každý prevádzkovateľ môže použiť iné otázky a formulácie pri posúdení nevyhnutnosti oprávneného záujmu.

Posledným krokom balančného testu je samotné **vyvažovanie (test proporcionality v užšom zmysle).** V tomto kroku ide o pomerne náročné právne cvičenie vyvažovania oprávneného záujmu voči právam, slobodám a záujmom dotknutých osôb. Proporcionalita laicky znamená, že opatrenia, ktoré zasahujú do práv a právom chránených záujmov dotknutých osôb, sú

[108] European Data Protection Supervisor . Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit. Dostupné na https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.
[109] K tomu pozri napr. HUDECOVÁ, I. – CYPRICHOVÁ, A. – MAKATURA, I. a kol.: *Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár*. Eurokódex, 2018, s. 160 a nasl. a Usmernenie ICO. Dostupné na https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx.
[110] K tomu European Data Protection Supervisor. Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit. Dostupné na https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

vhodné a najmenej invazívne, ako je možné[111]. Samotné vyvažovanie môže mať rôzne podoby – súvislý právny text, *Q & A* (otázky a odpovede) alebo test s bodovým ohodnotením.

Britský ICO (*Information* Commissioner *Office* – dozorný orgán) túto časť balančného testu delí na tri oblasti[112]:

1. Charakter osobných údajov:
   - či spracúvanie osobných údajov obsahuje citlivé osobné údaje
   - či ide o kontextuálne spracúvanie citlivých osobných údajov (tzn. že nejde o spracúvanie citlivých osobných údajov v zmysle článku 9 ods. 1 GDPR, ale z kontextu spracúvania vyplývajú citlivé informácie o dotknutých osobách, napr. údaje o polohe alebo údaje o finančnej situácii dotknutej osoby)
   - či sa osobné údaje týkajúce zraniteľných osôb (napr. deti, dôchodcovia, zdravotne postihnutí) alebo verejne exponovaných osôb (verejní funkcionári či umelci).
2. Primerané očakávania dotknutých osôb:
   - či dotknuté osoby môžu legitímne očakávať spracúvanie osobných údajov na daný účel
   - spôsob spracúvania osobných údajov (profilovanie alebo automatizované individuálne rozhodovanie, zverejňovanie osobných údajov)
   - aký je vzťah medzi prevádzkovateľom a dotknutou osobou
   - či boli osobné údaje získané priamo alebo nepriamo od dotknutých osôb
   - ako dlho boli osobné údaje získavané
   - či obsahuje spracúvanie osobných údajov novú technológiu alebo inováciu.

[111] Tamže, s. 9.
[112] Usmernenie ICO. Dostupné na https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

3. Potenciálny vplyv:
    - analýza potenciálnej škody pre prevádzkovateľa pri nevykonaní spracúvania osobných údajov
    - posúdenie negatívnych vplyvov na dotknuté osoby/tretie strany
    - posúdenie pozitívnych vplyvov na dotknuté osoby/tretie strany
    - relevantný prínos pre prevádzkovateľa
    - relevantný prínos pre dotknutú osobu/tretie strany
    - či prevádzkovateľ implementoval záruky na ochranu práv dotknutých osôb (technické alebo organizačné opatrenia).

V prípade, ak je výsledok balančného testu pozitívny, prevádzkovateľ by ho mal zdokumentovať a môže na tomto právnom základe spracúvať osobné údaje na daný účel. Typicky sa oprávnený záujem ako právny základ používa pri monitorovaní priestorov kamerovým systémom alebo na niektoré marketingové účely.

Avšak tento právny základ je možné využiť aj v rámci pracovnoprávnych vzťahov.[113] Pracovná skupina článku 29 zvýrazňuje, že pri využití právneho základu oprávneného záujmu v pracovnoprávnych vzťahoch je nevyhnutné implementovať opatrenia na zmiernie zásahov do práv, slobôd a záujmov dotknutých osôb.[114] Takéto opatrenia môžu predstavovať limitovanie spracúvania osobných údajov z hľadiska geografického rozsahu (iba na špecifickom mieste), rozsahu údajov (iba špecifický typ údajov) alebo času (iba časové pečiatky namiesto kontinuálneho monitorovania).[115] V zmysle vyššie uvedených odporúčaní by preto zlú prax predstavovalo:

- Neustále monitorovania polohy zamestnanca,

[113] ARTICLE 29 DATA PROTECTION WORKING PARTY: Opinion 2/2017 on data processing at work, 17/EN WP 249, s. 7 a nasl.
[114] ARTICLE 29 DATA PROTECTION WORKING PARTY: Opinion 2/2017 on data processing at work, 17/EN WP 249, s. 7.
[115] ARTICLE 29 DATA PROTECTION WORKING PARTY: Opinion 2/2017 on data processing at work, 17/EN WP 249, s. 8.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

- Monitorovanie zamestnanca aj počas prestávky na odpočinok alebo mimo pracovného času
- Monitorovanie súkromnej komunikácie.

Vyššie uvedené činnosti by len veľmi ťažko prešli testom prevahy oprávneného záujmu.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

3 OCHRANA OSOBNÝCH ÚDAJOV ZAMESTNANCA PODĽA ZÁKONA O OCHRANE OSOBNÝCH ÚDAJOV

3.1 VZÁJOMNÉ INTERAKCIE MEDZI ZÁKONOM O OCHRANE OSOBNÝCH ÚDAJOV A GDPR

GDPR predstavuje unifikáciu pravidiel na ochranu osobných údajov na úrovni EÚ. Vzhľadom na to, že staršia smernica 95/46/ES bola v jednotlivých členských štátoch implementovaná rôznymi spôsobmi, nedosiahla sa požadovaná rovnaká alebo podobná úroveň ochrany osobných údajov na starom kontinente.[116] Aj vzhľadom na dynamický technologický vývoj, globalizáciu, kvantum cezhraničných prenosov či zverejňovanie množstva údajov fyzickými osobami na internetovej sieti sa EÚ rozhodla pre súdržnejší právny rámec v podobe nariadenia.[117] *„Tento vývoj si vyžaduje silný a súdržnejší rámec ochrany údajov v Únii, ktorý sa bude intenzívne presadzovať vzhľadom na význam vybudovania dôvery, ktorá umožní rozvoj digitálnej ekonomiky v rámci vnútorného trhu. Fyzické osoby by mali mať kontrolu nad svojimi vlastnými osobnými údajmi. Mala by sa posilniť právna a praktická istota pre fyzické osoby, hospodárske subjekty a orgány verejnej moci.“*[118] GDPR však zároveň umožňuje, aby právo členského štátu spresnilo alebo obmedzilo ustanovené pravidlá v presne vymedzených prípadoch.[119] Vo väčšine prípadov ide o špecifikáciu konkrétnych otázok, na ktorých sa členské štáty EÚ nevedeli zhodnúť pri negociovaní finálneho znenia nariadenia.[120] Vzhľadom na množstvo takýchto ustanovení je však možné, že právna úprava ochrany osobných údajov v jednotlivých členských štátoch bude opäť časom značne diverzifikované a nebude reflektovať cieľ súdržnejšieho právneho rámca.

Vo všeobecnosti existujú tri možnosti vlastnej úpravy resp. spresnenia ustanovení GDPR v rámci mantinelov poskytnutých týmto nariadením. Dve možnosti sú legislatívneho charakteru a teda priamo v rukách národných zákonodarných orgánov. Tretia možnosť je

---

[116] Recitál 9 GDPR.
[117] Recitál 6 GDPR.
[118] Recitál 7 GDPR.
[119] Recitál 8 GDPR: „Ak sa v tomto nariadení stanovuje, že právo členského štátu má spresniť alebo obmedziť jeho pravidlá, členské štáty môžu, pokiaľ je to nevyhnutné pre súdržnosť a dosiahnutie lepšej zrozumiteľnosti vnútroštátnych predpisov pre osoby, na ktoré sa vzťahujú, začleniť prvky tohto nariadenia do svojho vnútroštátneho práva.“
[120] FEILER, L. – FORGÓ, N. – WEIGL, M.: *The EU General Data Protection Regulation (GDPR): A Commentary.* Globe Law and Business, 2018, s. 30.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

prostredníctvom samoregulačného nástroja v špecifických sektoroch, kde má však štát možnosť apelácie a nepriameho ovplyvnenia prostredníctvom dozorných orgánov resp. členstva v orgánoch inštitúcií EÚ. Tieto tri možnosti predstavujú:

1. Využitie otvorených klauzúl (*Opening clauses*);
2. Derogácia GDPR v zmysle článku 23 GDPR; a
3. Samoregulačné nástroje.

3.1.1 Otvorené klauzuly

Otvorené klauzuly v GDPR sú dôsledkom toho, že členské štáty EÚ pri tvorbe a prijímaní nariadenia nevedeli nájsť konsenzus v určitých špecifických otázkach. Výsledkom tak je, že niektoré ustanovenia GDPR umožňujú mieru flexibility pri ich zapracovaní do právnych poriadkov členských štátov EÚ. Ako jeden z príkladov je možné uviesť problematiku ustanovenia veku dieťaťa v súvislosti s digitálnym súhlasom podľa článku 8 GDPR. V tejto oblasti je kultúra jednotlivých členských štátov natoľko rozdielna, že nebolo možné nájsť jednotný prístup a GDPR tak umožňuje stanoviť túto hranicu od 13 do 16 rokov.[121]

GDPR obsahuje celkovo **69 otvorených klauzúl**[122] rôznej kvality, ktoré umožňujú ustanovenie špecifikovať, doplniť alebo nahradiť v rámci národného právneho poriadku. Vzhľadom na počet otvorených klauzúl si dovoľujeme na tomto mieste uviesť iba kategorizovaný rámcový prehľad predmetných možnosti vlastnej právnej úpravy členských štátov.

V rámci základných definícií môžu členské štáty vo svojich právnych poriadkoch ustanoviť postavenie prevádzkovateľa pre konkrétne subjekty či postavenie orgánov verejnej moci ako príjemcov osobných údajov. V súvislosti s právnymi základmi členské štáty môžu kreovať zákonné povinnosti a úlohy vo verejnom záujme. V tomto kontexte osobitne upozorňujem na

[121] K danej problematike pozri napríklad Pozri MACENAINTE, M. – KOSTA, E.: Consent for processing children´s personal data in the EU: following in US footsteps? In *Information & Communications Technology Law*, 26:2, s. 145 – 197 alebo BUITELAAR, J.C.: Child´s Best Interest and Informational Self-Determination: What the GDPR can learn from children´s rights. In *International Data Privacy Law*, 2018, Vol. 8, No. 4, s. 293 – 308.

[122] FEILER, L.: *Öffnungsklauseln in der Datenschutz-Grundverordnung - Regelungsspielraum des österreichischen Gesetzgebers*. Dostupné na: https://lesen.lexisnexis.at/_/oeffnungsklauseln-in-der-datenschutz-grundverordnung-regelungssp/artikel/jusit/2016/5/jusIT_2016_05_093.html.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

možnosť zakotvenia koncepčného uchopenia kreovania týchto právnych základoch v práve členských štátoch.[123] Ako už bolo spomenuté vyššie, členské štáty môžu ručiť vek dieťaťa v súvislosti s digitálnym súhlasom.

Pomerne veľa otvorených klauzúl obsahuje článok 9 GDPR, ktorý sa týka spracúvania citlivých osobných údajov. V rámci druhého odseku sú totiž ustanovené situácie, v ktorých môžu národné právne poriadky ustanoviť výnimky, v ktorých je spracúvanie citlivých osobných údajoch povolené, konkrétne zákaz výslovného súhlasu v zákonom stanovených prípadoch, spracúvanie **v oblasti pracovného práva**, **sociálneho zabezpečenia** a poistenia, spracúvanie v oblasti medicíny a na základe významného verejného záujmu či dôvodu verejného zdravia. Osobitne možno taktiež upraviť spracúvanie na účel archivácie, vedeckých alebo historických účelom a štatistiky a určiť podmienky a obmedzenie spracúvania genetických, biometrických a údajov o zdravotnom stave. Podobne možno nastaviť v národnom právnom poriadku spracúvanie údajov týkajúcich sa uznania viny za trestné činy a priestupky.

V súvislosti s právami dotknutých osôb GDPR umožňuje členským štátom upraviť výnimky z plnenia informačnej povinnosti, práva na vymazanie (prípadne úpravu zákonnej povinnosti vymazania údajov) a povolenia automatizovaného individuálneho rozhodovania v zmysle článku 22 GDPR.

Inštitúty spoločných prevádzkovateľov (článok 26 GDPR) a sprostredkovateľov (článok 28 GDPR) je taktiež možné v národnom právnom poriadku špecifikovať s ohľadom na vymedzenie konkrétnych povinnosti spoločných prevádzkovateľov a dezignovanie sprostredkovateľa prostredníctvom zákonnej povinnosti prípadne atribútov spracúvania osobných údajov sprostredkovateľom[124] či určenia sub-sprostredkovateľa.

Osobitnou otvorenou klauzulou v súvislosti s inštitútom posúdenia vplyvu na ochranu údajov je možnosť členského štátu vykonať dané posúdenie v súvislosti s kreovaním právneho

[123] Článok 6 ods. 2 GDPR: „Členské štáty môžu zachovať alebo **zaviesť špecifickejšie ustanovenia** s cieľom prispôsobiť uplatňovanie pravidiel tohto nariadenia s ohľadom na spracúvanie v súlade s odsekom 1 písm. c) a e), a to **presnejším stanovením osobitných požiadaviek na spracúvanie a stanovením ďalších opatrení, ktorými sa zaistí zákonné a spravodlivé spracúvanie, vrátane požiadaviek na iné osobitné situácie spracúvania stanovené v kapitole IX.**“
[124] K tomu pozri článok 28 ods. 3 GDPR.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

základu zákonnej povinnosti alebo úlohy vo verejnom záujme. Národné právne poriadky taktiež môžu určiť, kedy je prevádzkovateľ povinný vykonať predchádzajúcu konzultáciu[125] či určiť zodpovednú osobu.[126]

V kontexte cezhraničných prenosov osobných údajov do tretích krajín môžu členské štáty upraviť viaceré výnimky pre cezhraničné prenosy v zmysle článku 49 GDPR a to konkrétne prenosy na základe verejného záujmu, pri prenose osobných údajov do tretej z registra poskytujúceho informácie verejnosti alebo naopak, prenosy na základe verejného záujmu obmedziť.

Množstvo otvorených klauzúl sa týka kreovania jedného alebo viacerých dozorných orgánov v členskom štáte EÚ. GDPR predovšetkým zvýrazňuje nevyhnutnosť vlastných zdrojov a jeho nezávislosť (vrátane finančnej nezávislosti). Ďalšie ustanovenia, ktoré si členské štáty majú upraviť sami sa týkajú vedúcich funkcií v rámci dozorného orgánu a to z hľadiska potrebnej kvalifikácie, procesu voľby, trvania funkcie a výmeny. GDPR taktiež umožňuje špecifikovať povinnosti a pracovné podmienky členov dozorných orgánov a upravenie povinnosť zachovávať mlčanlivosť pre členov dozorných orgánov. Dozorné orgány zároveň nie sú príslušné vykonávať dozor pri spracovateľských operáciách na súdoch pri výkone súdnej právomoci a preto členské štáty musia určiť kompetentný orgán na výkon predmetného dozoru. Ďalej je nutné upraviť poradné právomoci dozorných orgánov, ďalšie oprávnenia vrátanie podmienok pre vstup do priestorov prevádzkovateľa a sprostredkovateľa, pravidlá pre prenos oprávnení na iný dozorný alebo inšpekčný orgán či určenie subjektov, ktoré dostávajú správu o ochrane osobných údajov. V práve členského štátu sa ďalej môže upraviť právo neziskových organizácií podať sťažnosť nezávislé od dotknutých osôb. Obmedziť je možné aj sankcionovania orgánov verejnej moci.

Najviditeľnejšie otvorené klauzuly upravuje kapitola IX. GDPR, na základe ktorej si členské štáty môžu vytvárať rôzne zákonné povinnosti v súvislosti so spracúvaním osobných údajov a špecifikovať ich s ohľadom na národnú právnu kultúru. Ide konkrétne o otázky vyváženia práva na ochranu osobných údajov a slobody prejavu a práva na informácie, spracúvania na

[125] Článok 36 ods. 5 GDPR.
[126] Článok 37 ods. 4 GDPR.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

žurnalistické, akademické a umelecké účely, prístup verejnosti k dokumentom, spracúvanie rodných čísel, **spracúvanie údajov v pracovnoprávnych vzťahoch** alebo špecifík spracúvania údajov na štatistické, historické, vedecké a archívne účely.

Otvorenú klauzulu v kontexte spracúvania v súvislosti so zamestnaním upravuje článok 88 ods. GDPR: „Členské štáty môžu prostredníctvom právnych predpisov alebo kolektívnych dohôd **stanoviť konkrétnejšie pravidlá na zabezpečenie ochrany práv a slobôd pri spracúvaní osobných údajov zamestnancov v súvislosti so zamestnaním**, najmä na účely prijatia do zamestnania, plnenia pracovnej zmluvy vrátane plnenia povinností vyplývajúcich z právnych predpisov alebo kolektívnych zmlúv, ďalej na účely riadenia, plánovania a organizácie práce, rovnosti a rozmanitosti na pracovisku, ochrany zdravia a bezpečnosti pri práci, ochrany majetku zamestnávateľa alebo zákazníka, ako aj na účely uplatňovania a využívania práv a výhod súvisiacich so zamestnaním na individuálnom alebo kolektívnom základe, a na účely ukončenia pracovného pomeru.“ Tieto pravidlá však musia napĺňať literu požiadavky, aby reflektovali „vhodné a osobitné opatrenia na zaistenie ľudskej dôstojnosti, oprávnených záujmov a základných práv dotknutej osoby.“[127]

Národné právne poriadky taktiež môžu upraviť špecificky postup dozorných orgánov a ich oprávnení dozorných orgánov pri osobách s povinnosťou zachovávať mlčanlivosť (napríklad advokáti) a určiť nezávislý dozorný orgán pre cirkvi a náboženské spoločnosti.

Ako z vyššie uvedeného stručného prehľadu vyplýva, otvorené klauzuly reprezentujú rôznorodú skupinu ustanovení, na základe ktorých je možné postaviť národné právne úpravy.

3.1.1.1 Derogácia GDPR podľa článku 23 GDPR

Derogácie v zmysle článku 23 predstavujú špecifický prípad otvorenej klauzuly a z tohto dôvodu považujem za vhodné ich od seba oddeliť, nakoľko na seba viažu niekoľko rôznych dodatočných povinností. Článok 23 reflektuje fakt, že právo na ochranu osobných údajov nie je právom absolútnym a za určitých okolností ho možno obmedziť.

[127] Článok 88 ods. 2.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Základným rozdielom medzi derogáciou podľa článku 23 GDPR a inými otvorenými klauzulami je ten, že kým otvorené klauzuly všeobecne poskytujú určité mantinely na vlastnú právnu úpravu v určitých otázkach spracúvania osobných údajov, článok 23 GDPR ustanovuje možnosť členským štátom z precízne vymedzených dôvodov priamo obmedziť uplatňovanie určitých ustanovení GDPR.

Nakoľko predmetné derogácie možno uplatniť iba vo výnimočných situáciách ako je národná bezpečnosť, obrana alebo ochrana súdnictva a nezávislých inštitúcií, nebudeme tieto možnosti vzhľadom na predmet predkladanej štúdie hlbšie analyzovať.

3.1.1.2 Samoregulačné nástroje

Samoregulačné nástroje v rámci GDPR sú poslednou z možností, ako je možné spresniť výklad ustanovení GDPR. Ide však o veľmi špecifickú možnosť, ktorá sa týka spresnenia pravidiel spracúvania osobných údajov v konkrétnom sektore alebo pre konkrétne subjekty. Využitie týchto inštitútov tak nie je limitované na súkromný alebo verejný sektor.

Najvýznamnejším samoregulačným nástrojom sú kódexy správania (Code of Conducts) podľa článku 40 GDPR. V zmysle článku 40 ods. 1 GDPR: „Členské štáty, dozorné orgány, výbor a Komisia podporia vypracovanie kódexov správania určených na to, aby prispeli k správnemu uplatňovaniu tohto nariadenia, pričom vezmú do úvahy osobitné črty rôznych sektorov spracúvania a osobitné potreby mikropodnikov a malých a stredných podnikov.“

Kódexy správania sú záväzné dokumenty, ktoré regulujú spracúvanie osobných údajov v určitom segmente alebo sektore a môžu tak zohľadniť špecifické potreby daného prostredia. Ako príklad možno uviesť spracúvanie osobných údajov bankami, advokátmi, poisťovňami alebo v telekomunikačnom sektore. Výhodou takéhoto riešenia je odbornosť a vedomosti o špecifikách daného sektora zo strany tvorcov kódexu správania. V prípade, ak si daná organizácia takýto kódex navrhne, je povinná ho predložiť na schválenie kompetentnému dozornému orgánu, ktorý následne posúdi jeho súlad s pravidlami na ochranu osobných

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

údajov.[128] V prípade, ak kódex upravuje spracovateľské operácie vo viacerých členských štátoch EÚ, dozorný orgán požiada o vyjadrenie názoru aj Výbor na ochranu údajov.

Dôležitým aspektom kódexu správania je, že jednotliví členovia daného sektora sa musia zaviazať v prípade schválenia daný kódex dodržiavať. S tým súvisí aj povinnosť kreovať tzv. monitorujúci subjekt,[129] ktorý dodržiavanie kódexu správania bude monitorovať. Tento subjekt je povinný získať od dozorného orgánu akreditáciu na monitorovanie kódexu správania.

Jednotlivé členské štáty môžu v rámci národných právnych úprav apelovať na prijatie kódexov správania pre určité sektory alebo subjekty. Ako príklad možno uviesť írsku právnu úpravu, ktorá vyzýva na prijatie kódexu správania pre spracúvanie osobných údajov údajov detí za účelom zvýšenia ich právnej ochrany. § 32 *Data Protection Act 2018* ustanovuje povinnosť pre dozorný orgán podporovať tvorbu takýchto kódexov.

Vzhľadom na vyššie uvedené, nie je vylúčené, že aby zákonodarca priamo podporoval vznik kódexov správania týkajúcich sa pracovnoprávnych vzťahov alebo špecificky stanovil pravidlá pre vybrané spracovateľské operácie v rámci pracovnoprávnych vzťahov.

3.2 APLIKAČNÉ PROBLÉMY

Slovenská právna úprava v súvislosti s požiadavkami GDPR je reprezentovaná zákonom č. 18/2018 Z.z o ochrane osobných údajov (ďalej len „ZOOÚ“). Ide o štvrtý samostatný zákon o ochrane osobných údajoch v dejinách Slovenskej republiky. V rámci tejto časti načrtneme jeho štruktúru, pôsobnosť a využitie otvorených klauzúl.[130]

ZOOÚ je zložený zo šiestich častí a obsahuje dovedna 112 §§. Pre porovnanie, GDPR obsahuje 99 článkov, český zákon o ochrane osobných údajov[131] obsahuje 68 §§ a nemecký zákon o ochrane osobných údajov[132] obsahuje 86 §§. Samotná dĺžka zákona by nebola *a priori*

[128] Článok 40 ods. 5 GDPR.
[129] Pozri článok 41 GDPR.
[130] K legislatívnemu vývoju zákona o ochrane osobných údajov pozri MESARČÍK, M.: Slovakia. On the way to accountability? In *European Data Protection Law Review*, 4/2019, s. 537 – 543.
[131] Zákon č. 110/2019 Sb. O ochrane osobních údaju.
[132] Bundesdatenschutzgesetz.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

problémom, avšak drvivú časť ustanovení tvoria doslova a do písmená skopírované legálne znenia z GDPR (§ 6 – 51 ZOOÚ), vzhľadom na komplikovanú pôsobnosť našej právnej úpravy.

Prvá časť ZOOÚ upravuje základné ustanovenia týkajúce sa predmetu, pôsobnosti a definícií slovenskej právnej úpravy.

Druhá časť s názvom *„Všeobecné pravidlá ochrany osobných údajov fyzických osôb pri ich spracúvaní“* obsahuje duplicitné ustanovenia pre spracúvanie osobných údajov doslova prevzaté z GDPR.

Tretia časť ZOOÚ upravuje osobitné pravidlá ochrany osobných údajov fyzických osôb pri ich spracúvaní príslušnými orgánmi. Predmetná časť implementuje smernicu Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV, ktorá upravuje špecifická spracúvania príslušných orgánov (Policajný zbor, Vojenská polícia, Zbor väzenskej a justičnej stráže, Finančná správa, prokuratúra a súdy) pri tzv. trestnoprávnych účeloch - účely predchádzania a odhaľovania trestnej činnosti, zisťovania páchateľov trestných činov, stíhania trestných činov alebo na účely výkonu rozhodnutí v trestnom konaní vrátane ochrany pred ohrozením verejného poriadku a predchádzania takémuto ohrozeniu.

Štvrtá časť ZOOÚ obsahuje osobitné situácie zákonného spracúvania osobných údajov a ide o využitie otvorených klauzúl podľa kapitoly IX. GDPR. Táto právna úprava je však veľmi stručná (iba § 78 a § 79) a konkrétne situácie upravuje iba jednou alebo dvoma vetami.

Piata časť ZOOÚ sa týka slovenského dozorného orgánu – Úradu na ochranu osobných údajov SR a upravuje jeho postavenie, výkon kontroly, správne konanie a otázky súvisiace s predsedom dozorného orgánu SR. Šiestu časť tvoria spoločné, prechodné a záverečné ustanovenia.

Pôsobnosť ZOOÚ je vymedzená v § 3. Z tohto pohľadu sú dôležité ustanovenia § 3 ods. 2 a 3, ktoré ustanovujú, že „tento zákon, okrem § 2, § 5, druhej a tretej časti zákona, sa vzťahuje na spracúvanie osobných údajov, na ktoré sa vzťahuje osobitný predpis o ochrane fyzických osôb

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov“ (GDPR) a pre spracúvanie osobných údajov príslušnými orgánmi „sa (tento zákon) vzťahuje na spracúvanie osobných údajov Policajným zborom, Vojenskou políciou, Zborom väzenskej a justičnej stráže, Finančnou správou, prokuratúrou a súdmi (ďalej len „príslušný orgán“) na účely predchádzania a odhaľovania trestnej činnosti, zisťovania páchateľov trestných činov, stíhania trestných činov alebo na účely výkonu rozhodnutí v trestnom konaní vrátane ochrany pred ohrozením verejného poriadku a predchádzania takémuto ohrozeniu (ďalej len „plnenie úloh na účely trestného konania“); z druhej časti tohto zákona sa na spracúvanie osobných údajov podľa predchádzajúcej časti vety vzťahujú len ustanovenia uvedené v § 52, § 59, § 67 a § 73.“

Už pri pripomienkovaní návrhu daného zákona smerovalo viacero pripomienok ku nezrozumiteľnosti a rozpornosti ohľadom pôsobnosti. Vyššie uvedené ustanovenia pôsobili v praxi značne zmätočne a preto Úrad na ochranu osobných údajov SR[133] vo svojom metodickom usmernení vymedzil tri modely pôsobnosti GDPR a ZOOÚ:

1. Ak pôjde o spracúvanie osobných údajov v rámci činnosti prevádzkovateľa, ktorá **spadá pod právo Európskej únie**, tak sa v zásade aplikuje GDPR + štvrtá časť a ustanovenia týkajúce sa činnosti dozorného orgánu podľa ZOOÚ;
2. Ak pôjde o spracúvanie osobných údajov v rámci činností prevádzkovateľa, ktoré **nespadajú pod právo EÚ**, tak sa aplikuje iba ZOOÚ s výnimkou tretej časti;
3. V prípade spracúvania osobných údajov príslušnými orgánmi na plnenie úloh na účely trestného konania sa aplikuje tretia časť ZOOÚ a presne vymedzené ustanovenia druhej časti spolu so štvrtou, piatou a šiestou časťou nášho zákona.

Kritériom pre určenie pôsobnosti teda vo väčšine prípadov bude to, či spracovateľské operácie patria alebo nepatria do pôsobnosti práva EÚ. Právo EÚ však v zakladajúcich zmluvách nevymedzuje negatívnu pôsobnosť a teda oblasti, v ktorých nemá právomoc. Práve naopak, derivovať možno iba oblasti, v ktorých Európska únia právomoci má a preto je veľmi náročné

[133] Úrad na ochranu osobných údajov SR: *Kedy zákon a kedy nariadenie?* Dostupné na: https://dataprotection.gov.sk/uoou/sites/default/files/kedy_zakon_kedy_nariadeniepdff.pdf (dostupné 1.8.2020).

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

poskytnúť prehľad oblastí, kde EÚ právomoc nemá. Navyše, SDEÚ nedávno judikoval, že oblasti, ktoré patria do výlučnej právomoci členských štátov EÚ v kontexte ochrany osobných údajov je potrebné interpretovať reštriktívne.[134] Dôvodom pre zakotvenie pravidiel pre spracúvanie osobných údajov, ktoré nespadajú pod právo EÚ mala byť právna istota a pokrytie spracovateľských operácií, ktoré by pôsobnosti práva EÚ unikli.[135]

Z vyššie uvedeného tak možno vyvodiť, že na väčšinu entít spracúvajúcich osobné údaje sa bude vzťahovať prvý režim, keďže to budú činností, ktoré spadajú pod právo EÚ. Zároveň je potrebné poznamenať, že otázky komplikovanej pôsobnosti kritizoval aj Národný kontrolný úrad vo svojej Záverečnej správe - Systém ochrany a bezpečnosti údajov vo verejnom sektore z apríla 2020.[136]

ZOOÚ využíva viaceré otvorené klauzuly, avšak koncepčne to robí zvláštnym spôsobom. Reflexia otvorených klauzúl sa nachádza v troch častiach ZOOÚ. V prvom rade ide o klauzuly, ktoré upravujú postavenie a fungovanie Úradu na ochranu osobných údajov SR v piatej časti zákona. V druhom rade ide o využitie otvorených klauzúl z kapitoly IX GDPR, ktoré sa nachádza v štvrtej časti, konkrétne § 78 a § 79 ZOOÚ.[137] V treťom rade sa ustanovenia v mantineloch otvorených klauzúl nachádzajú aj v druhej časti ZOOÚ. Ide napríklad o určenie veku dieťaťa s digitálnym súhlasom (§ 15 ZOOÚ) alebo v stručnej forme parametre kreovania právneho základu v podobe zákonnej povinnosti alebo verejného záujmu (§ 6 ods. 2 ZOOÚ). V tomto smere je však potrebné poznamenať, že vzhľadom na pôsobnosť právnych aktov diskutovaných v predchádzajúcej stati bude v drvivej väčšine druhá časť ZOOÚ prakticky

[134] Pozri rozhodnutie SDEÚ z 9. júla 2020 C-272/19, *VQ proti Land Hesse*, body 66 – 74.
[135] Pozri Dôvodová správa k vládnemu návrhu zákona o ochrane osobných údajov. Dostupné na: https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=443222; a Úrad na ochranu osobných údajov SR: *Kedy zákon a kedy nariadenie?* Dostupné na: https://dataprotection.gov.sk/uoou/sites/default/files/kedy_zakon_kedy_nariadeniepdff.pdf.
[136] Národný kontrolný úrad SR: *Záverečná správa - Systém ochrany a bezpečnosti údajov vo verejnom sektore.* Bratislava: 2020. Dostupné na: https://www.nku.gov.sk/documents/10157/265201/96578-0-110.pdf, s. 17 a nasl, s. 22.
[137] „Štvrtá časť navrhovanej právnej úpravy vo svojich ustanoveniach je tzv. implementačnou/vykonávacou časťou zákona, ktorá dopĺňa osobitné pravidlá spracúvania osobných údajov stanovené nariadením.“ Dôvodová správa k vládnemu návrhu zákona o ochrane osobných údajov. Dostupné na: https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=443222.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

neaplikovateľná. Využitie otvorených klauzúl a ich zaradenie to tejto časti zákona je v konečnom dôsledku úplne zbytočné.

§ 78 ZOOÚ upravuje osobitné situácie zákonného spracúvania osobných údajov v podobe využitia otvorených klauzúl podľa kapitoly IX GDPR. Týchto osobitných situácií je celkovo sedem. Na niektorých miestach si dovoľujem znenie slovenských ustanovení komparovať s vybranými členskými štátmi EÚ.

Prvou situáciou sú akademické, umelecké, a literárne účely, pričom možnosť spracúvania údajov na dané účely je podmienená nevyhnutnosťou a legálnosťou.[138] Žiadne ďalšie detaily v kontexte vyváženia daných práv ZOOÚ neobsahuje. Rakúska právna úprava napríklad obsahuje precízny výpočet článkov GDPR, ktoré sa pri týchto účeloch neaplikujú.[139] Podobný prístup zachoval aj írsky zákonodarca[140] a český zákon o ochrane osobných údajov.[141]

Druhou situáciu je tzv. žurnalistická výnimka: „Prevádzkovateľ môže spracúvať osobné údaje bez súhlasu dotknutej osoby aj vtedy, ak spracúvanie osobných údajov je nevyhnutné pre potreby informovania verejnosti masovokomunikačnými prostriedkami a ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu činnosti.“[142] Opätovne platí podmienka nevyhnutnosti a legálnosti ako v predchádzajúcej situácií. Estónska právna úprava viaže využitie tejto výnimky na dodržiavanie princípov novinárskej etiky a verejného záujmu.[143]

Treťou situáciou je využitie otvorenej klauzuly v pracovnoprávnych vzťahoch. Zamestnávatelia môžu žiadať a zverejňovať vymedzené osobné údaje[144] od zamestnancov, ak je to potrebné v súvislosti s plnením pracovných povinností, služobných povinností alebo

[138] § 78 ods. 1 ZOOÚ: „To neplatí, ak spracúvaním osobných údajov na taký účel prevádzkovateľ porušuje právo dotknutej osoby na ochranu jej osobnosti alebo právo na ochranu súkromia alebo také spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná.“
[139] § 9 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG).
[140] § 43 Data Protection Act (Ireland) 2018.
[141] § 17 – 23 zákona č. 110/2019 Sb. O zpracování osobních údajú.
[142] § 78 ods. 2 ZOOÚ.
[143] § 4 Personal Data Protection Act. Passed 12.12.2018.
[144] Konkrétne titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresa elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

funkčných povinností dotknutej osoby. Predmetné spracovateľské operácie nesmú narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby. Pre porovnanie, nemecká právna úprava obsahuje precízne vymedzené pojmy zamestnanca, účelov, spracúvania na základe súhlasu a spracúvania citlivých osobných údajov v pracovnoprávnych vzťahoch.[145] Podobne, írska právna úprava osobitne chráni spracúvanie údajov týkajúcich sa zdravia zamestnancov.[146]

Štvrtá situácia sa týka spracúvania rodného čísla. Rodné číslo je možné spracúvať len vtedy, ak jeho využitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Ak je spracúvanie rodného čísla založené na výslovnom súhlase dotknutej osoby, nesmie danú spracovateľskú operáciu vylučovať osobitný predpis. Zverejňovať všeobecne použiteľný identifikátor sa zakazuje s výnimkou prípadov, ak všeobecne použiteľný identifikátor zverejní sama dotknutá osoba.

Piata situácia sa týka možnosti získania osobných údajov od inej fyzickej osoby a spracúvania v informačnom systéme len s predchádzajúcim písomným súhlasom dotknutej osoby.[147] Táto osobitná situácia predstavuje dokonalý relikt[148] staršieho zákona o ochrane osobných údajov, ktorý bol postavený na notifikačných povinnostiach ohľadom tzv. informačných systémov, ktoré neboli vykladané v súlade s právom EÚ, ale predstavovali akýkoľvek účel alebo skupinu spracovateľských operácií. Toto ustanovenie nemá v danom nastavení žiadny zmysel, keďže GDPR nevylučuje získanie osobných údajov od tretej osoby pri plnení zákonných povinností (viď napríklad článok 14 GDPR). Ani z dôvodovej správy nie je zrejmé, akú otvorenú klauzulu tu zákonodarca využíva. Z vyššie uvedených dôvodov je preto možné, že predmetné ustanovenie nie je v súlade s právom EÚ.

---

[145] § 26 Bundesdatenschutzgesetz.
[146] § 46 Data Protection Act (Ireland) 2018.
[147] § 78 ods. 6 ZOOÚ: „Osobné údaje o dotknutej osobe možno získať od inej fyzickej osoby a spracúvať v informačnom systéme len s predchádzajúcim písomným súhlasom dotknutej osoby; to neplatí, ak poskytnutím osobných údajov o dotknutej osobe do informačného systému iná fyzická osoba chráni svoje práva alebo právom chránené záujmy, oznamuje skutočnosti, ktoré odôvodňujú uplatnenie právnej zodpovednosti dotknutej osoby, alebo sa osobné údaje spracúvajú na základe osobitného zákona podľa § 13 ods. 1 písm. c) a e). Ten, kto také osobné údaje spracúva, musí vedieť preukázať úradu na jeho žiadosť, že ich získal v súlade s týmto zákonom.“
[148] K tomu pozri aj výklad tohto ustanovenia v publikácií VALENTOVÁ, T. – BIRNSTEIN, M. – GOLAIS, J.: *GDPR/Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov. Praktický komentár.* Bratislava: Wolters Kluwer, 2018, s. 440 – 441.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Šiesta situácia upravuje spracúvanie osobných údajov zosnulých osôb. „Ak dotknutá osoba nežije, súhlas vyžadovaný podľa tohto zákona alebo osobitného predpisu môže poskytnúť jej blízka osoba. Súhlas nie je platný, ak čo len jedna blízka osoba písomne vyslovila nesúhlas.“ Estónska právna úprava viaže platnosť súhlasu zosnulých osôb na konkrétne lehoty (10 – 20 rokov) a v prípade potomkov, stačí ak súhlas so spracúvaním osobných údajov udelí čo i len jeden z nich. Zároveň estónsky zákon upravuje možnosť spracúvať konkrétne osobné údaje zosnulej osoby na účely smútočného oznámenia a vykonania pohrebu.[149] Podobný prístup zvolilo Maďarsko, Írsko alebo Dánsko.

Siedmou situáciou je spracúvanie na účely archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, pričom v daných prípadoch je prevádzkovateľ povinný prijať primerané záruky pre práva dotknutej osoby. Tieto záruky obsahujú zavedenie primeraných a účinných technických a organizačných opatrení a ZOOÚ výslovne spomína zabezpečenie dodržiavania zásady minimalizácie údajov a pseudonymizácie. *De facto* však v tomto prípade ide iba o skopírovanie požiadaviek z článku 89 ods. 1 GDPR.[150] § 78 ods. 9 ZOOÚ zároveň umožňuje obmedziť niektoré práva dotknutých osôb na dané účely *„osobitným predpisom alebo medzinárodnou zmluvou, ktorou je Slovenská republika viazaná, ak sú prijaté primerané podmienky a záruky podľa odseku 6, ak by tieto práva dotknutej osoby pravdepodobne znemožnili alebo závažným spôsobom sťažili dosiahnutie týchto účelov a také obmedzenie práv dotknutej osoby je nevyhnutné na dosiahnutie týchto účelov.“* V danom ustanovení zákonodarca opäť len skopíroval znenie z článku 89 ods. 2 GDPR a ani sa neunúval opraviť odkaz na predchádzajúci odsek (zjavne mal na mysli odsek 7 a nie 8).[151] Totožné závery a konštatovania platia aj v prípade využitia otvorenej klauzuly na účely archivácie v zmysle § 78 ods. 10 ZOOÚ. Reflexia diskutovaných otvorených klauzúl je v porovnaní s inými členskými

[149] § 9 Personal Data Protection Act. Passed 12.12.2018.
[150] Článok 89 ods. 1 GDPR: „Na spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely sa v súlade s týmto nariadením **vzťahujú primerané záruky pre práva a slobody dotknutej osoby. Uvedenými zárukami sa zaistí zavedenie technických a organizačných opatrení najmä s cieľom zabezpečiť dodržiavanie zásady minimalizácie údajov**.“
[151] Článok 89 ods. 2 GDPR: „Keď sa osobné údaje spracúvajú na účely vedeckého alebo historického výskumu či na štatistické účely, v práve Únie alebo v práve členského štátu sa môžu stanoviť odchýlky z práv uvedených v článkoch 15, 16, 18 a 21, pričom sa dodržia podmienky a záruky uvedené **v odseku 1 tohto článku**, pokiaľ takéto práva pravdepodobne znemožnia alebo závažným spôsobom sťažia dosiahnutie osobitných účelov, a takéto odchýlky sú nevyhnutné na dosiahnutie uvedených účelov.“

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

štátmi EÚ veľmi slabá. Rakúska právna úprava obsahuje podrobný výpočet podmienok pre spracúvanie osobných údajov na tieto účely, možnosť dozorného orgánu spracúvanie v určitých situáciách povoliť (napríklad pri vedeckých projektoch, kde je nemožné získať súhlas dotknutej osoby), požiadavku významného verejného záujmu pri spracúvaní citlivých osobných údajov alebo šifrovania údajov v rôznych fázach vedeckého výskumu.[152] Podrobne koncipovaná je aj estónska právna úprava.[153] Český zákon o ochrane osobných údajov vymenúva rôzne povinnosti aj s ohľadom na informačnú bezpečnosť pri spracúvaní daných údajov.[154]

GDPR v článku 9 ods. 4 umožňuje, aby členské štáty upravili ďalšie podmienky vrátane obmedzení týkajúce sa spracúvania genetických údajov, biometrických údajov alebo údajov týkajúcich sa zdravia. Slovenský zákonodarca „podmienil" spracúvanie týchto údajov spôsobom, že ich prevádzkovatelia môžu spracúvať *aj* (!) na základe osobitných predpisov a medzinárodných zmlúv bez ďalšej špecifikácie.[155] Žiadne obmedzenie sa v danom ustanovení nenachádza.

Zároveň sa nepochopiteľne v ustanovení § 78 ods. 11 ZOOÚ nachádza požiadavka, v zmysle ktorej „prevádzkovateľ a sprostredkovateľ pri prijímaní bezpečnostných opatrení a pri posudzovaní vplyvu na ochranu osobných údajov postupuje primerane podľa medzinárodných noriem a štandardov bezpečnosti." V súvislosti s bezpečnosťou neobsahuje GDPR žiadnu otvorenú klauzulu a navyše dodržiavanie noriem a štandardov bezpečnosti nariadenie taktiež nepozná. Podľa môjho názoru dané ustanovenie ZOOÚ ide zásadne nad rámec dovoleného a porušuje právo EÚ, nakoľko obsahujú povinnosť, ktorá žiadnym spôsobom nemá oporu v GDPR. Neobstojí ani výklad, že táto povinnosť sa aplikuje na prevádzkovateľov v režime, kde

[152] § 7 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG).
[153] § 6 Personal Data Protection Act. Passed 12.12.2018.
[154] § 16 zákona č. 110/2019 Sb. O zpracování osobních údajů.
[155] § 78 ods. 5 ZOOÚ: „Prevádzkovateľ môže spracúvať genetické údaje, biometrické údaje a údaje týkajúce sa zdravia aj na právnom základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná."

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

nemá pôsobnosť právo EÚ,[156] nakoľko práve toto ustanovenie sa nachádza v časti, ktorá sa aplikuje aj v režime, kde spracovateľské operácie podliehajú právu EÚ.

Navyše, slovenský zákonodarca sa nerozhodol využiť viaceré otvorené klauzuly vôbec a v ZOOÚ tak napríklad absentuje legislatívne posúdenie vplyvu na ochranu údajov, určenie zodpovednej osoby nad rámec GDPR či povinnosť vykonať predchádzajúcu konzultáciu pre vymedzených prevádzkovateľov.

V konečnom dôsledku tak možno zhrnúť nasledovné. ZOOÚ má komplikovanú pôsobnosť a navyše úplne zbytočne kopíruje ustanovenia GDPR, čím vytvoril pre adresátov právnych noriem stav právnej neistoty, ktorú legislatívu aplikovať. Využitie otvorených klauzúl slovenským zákonodarcom možno kritizovať z dvoch dôvodov. Prvým je využitie niektorých otvorených klauzúl v druhej časti ZOOÚ, ktorá sa takmer nikdy aplikovať nebude. Druhým dôvodom je v niektorých prípadoch (a osobitne pri štvrtej časti ZOOÚ) veľmi stručná a často nič nehovoriaca právna úprava otvorených klauzúl. Tomu nasvedčuje aj využitie otvorených klauzúl v iných členských štátoch EÚ.

3.3 NÁVRHY DE LEGE FERENDA

Vzhľadom na vyššie uvedené máme za to, že ja na mieste otvoriť diskusiu o revízii právneho rámca na ochranu osobných údajov.

Z hľadiska štruktúry by slovenská právna úprava mala zachovať pôvodnú štruktúru. Navyše, iné členské štáty EÚ pristúpili ku koncipovaniu národných právnych úprav veľmi podobne. Jedinou zmenou je nahradenie druhej časti ZOOÚ (ktorá kopíruje ustanovenia GDPR) využitím otvorených klauzúl. Zároveň považujeme za vhodné aj zaradenie implementácie Policajnej smernice ako poslednú časť „hmotnoprávnej časti“ pred ustanoveniami týkajúcimi sa pôsobnosti a úloh a dozorného orgánu. Týmto krokom by prišlo ku oddeleniu vykonávacích ustanovení GDPR a implementácií Policajnej smernice.

[156] VALENTOVÁ, T. – BIRNSTEIN, M. – GOLAIS, J.: GDPR/Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov. Praktický komentár. Bratislava: Wolters Kluwer, 2018, s. 442.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Slovenská právna úprava by z hľadiska štruktúry mohla vyzerať nasledovne. Prvá časť by upravovala základné ustanovenia týkajúce sa predmetu, pôsobnosti a definícií slovenskej právnej úpravy. Druhá časť s pracovným názvom *„Spracúvanie osobných údajov v zmysle Všeobecného nariadenia o ochrane údajov“* by obsahovala v prvej kapitole využitie koncepčných otvorených klauzúl (ako napríklad kritéria na kreovanie právneho základu zákonnej povinnosti a verejného záujmu alebo legislatívne zakotvenie potreby posúdenia vplyvu či ďalšie prípady povinnosti ustanoviť zodpovednú osobu). Druhá kapitola druhej časti by bola tvorená osobitnými situáciami zákonného spracúvania osobných údajov po vzore zásadne doplneného § 78 ZOOÚ. Tretia časť by reflektovala implementáciu Policajnej smernice. Štvrtá časť by sa týkala slovenského dozorného orgánu – Úradu na ochranu osobných údajov SR a upravovala jeho postavenie, výkon kontroly, správne konanie a otázky súvisiace s predsedom dozorného orgánu SR. Piatu časť by tvorili spoločné, prechodné a záverečné ustanovenia.

Už v predchádzajúcej stati sme upozorňovali na prekomplikovanú pôsobnosť ZOOÚ. Podľa nášho názoru, ak chcel slovenský zákonodarca do pôsobnosti slovenského ZOOÚ zahrnúť aj spracovateľské operácie, ktoré nereguluje právo EÚ, mohol túto otázku vyriešiť aj jednoduchšie ako skopírovaním veľkého množstva ustanovení GDPR do našej právnej úpravy. Toto riešenie by spočívalo v ustanovení pôsobnosti slovenskej právnej úpravy aj na spracovateľské operácie, ktoré nepatria do pôsobnosti práva EÚ. Takýmto spôsobom danú otázku vyriešili viaceré členské štáty EÚ ako napr. Česká republika,[157] Veľká Británia,[158]

[157] § 4 ods. 2 zákona č. 110/2019 Sb. O zpracování osobních údajů: „Ustanovení této hlavy a nařízení Evropského parlamentu a Rady (EU) 2016/679 se použijí i při zpracování osobních údajů, které mají být nebo jsou zařazeny do evidence, a při zpracování osobních údajů, které probíhá zcela nebo částečně automatizovaně, nejde-li o zpracování osobních údajů fyzickou osobou v průběhu výlučně osobních nebo domácích činností,
a) při výkonu činností, které nespadají do oblasti působnosti práva Evropské unie nebo do působnosti hlavy III nebo IV, nebo
b) při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o Evropské unii.“

[158] § 22 ods. 1 Data Protection Act 2018: „The GDPR applies to the processing of personal data to which this Chapter applies but as if its Articles were part of an Act extending to England and Wales, Scotland and Northern Ireland.“

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Nemecko[159] alebo Rakúsko[160] a Maďarsko.[161] Domnievame sa, že takouto klauzulou by nedošlo ku porušeniu práva EÚ, nakoľko aj iné členské štáty EÚ zvolili totožný spôsob, ako sa s danou otázkou vysporiadať.

Máme za to, že po vzore nemeckej právnej úpravy by sa zákonodarca mohol inšpirovať pri využití otvorenej klauzuly v pracovnoprávnych vzťahoch. Nemal by sa zamerať iba na sprístupňovanie určitých údajov, ako to robí súčasný ZOOÚ, ale zohľadniť aj možnosti spracúvania údajov týkajúcich sa zdravia a ich okolností (hlavne z pohľadu šírenia nebezpečne nákazlivej choroby COVID-19) či možného monitorovania priestorov zamestnávateľa za účelom ochrany majetku a v tejto súvislosti aj vyjasnení limitov § 13 ods. 4 zákona č. 311/2001 Z. z. Zákonníka práce.

[159] § 1 ods. 8 Bundesdatenschutzgesetz: „Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten finden die Verordnung (EU) 2016/679 und die Teile 1 und 2 dieses Gesetzes entsprechend Anwendung, soweit nicht in diesem Gesetz oder einem anderen Gesetz Abweichendes geregelt ist."

[160] § 4 ods. 1 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG): „Die Bestimmungen der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016 S. 1, (im Folgenden: DSGVO) und dieses Bundesgesetzes gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten natürlicher Personen sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten natürlicher Personen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, soweit nicht die spezifischeren Bestimmungen des 3. Hauptstücks dieses Bundesgesetzes vorgehen."

[161] § 3 ods. 5 011. évi CXII. Törvény az információs önrendelkezési jogról és az információszabadságról: „Személyes adatoknak az általános adatvédelmi rendelet hatálya alá tartozó kezelésére e törvény a (2) bekezdésben meghatározott rendelkezéseit, valamint más, törvényben meghatározott, a személyes adatok védelmére és a személyes adatok kezelésének feltételeire vonatkozó előírásokat – ha törvény vagy az Európai Unió kötelező jogi aktusa másként nem rendelkezik..."

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

4 OCHRANA OSOBNÝCH ÚDAJOV A SÚKROMIA ZAMESTNANCA V PREDZMLUVNÝCH VZŤAHOCH

4.1 PRÁVO NA PRÍSTUP K ZAMESTNANIU

Služby zamestnanosti sú inštitútom, ktorým je zákonným vyjadrením práva na prácu, ktorého realizácia spočíva v pozitívnom záväzku štátu zabezpečiť jeho realizáciu. V tomto zmysle zákon o službách zamestnanosti definuje v § 14 pojem právo na prístup k zamestnaniu, pod ktorým rozumieme právo občana, ktorý chce pracovať, môže pracovať a hľadá zamestnanie, na služby podľa tohto zákona zamerané na pomoc a podporu uľahčenia jeho vstupu na trh práce vrátane pomoci a podpory vstupu a zotrvania znevýhodneného uchádzača o zamestnanie na trhu práce najmenej počas obdobia šiestich po sebe nasledujúcich kalendárnych mesiacov.

Občania majú právo na prístup k zamestnaniu bez akýchkoľvek obmedzení v súlade so zásadou rovnakého zaobchádzania v pracovnoprávnych vzťahoch a obdobných právnych vzťahoch, pričom v súlade s touto zásadou sa zakazuje diskriminácia aj z dôvodu manželského stavu a rodinného stavu, farby pleti, jazyka, politického alebo iného zmýšľania, odborovej činnosti, národného alebo sociálneho pôvodu, zdravotného postihnutia, veku, majetku, rodu alebo iného postavenia a zároveň uplatňovanie práv a povinností vyplývajúcich z práva na prístup k zamestnaniu musí byť v súlade s dobrými mravmi. Nikto nesmie tieto práva a povinnosti zneužívať na škodu druhého občana. Nikto nesmie byť v súvislosti s uplatňovaním práva na prístup k zamestnaniu prenasledovaný ani inak postihovaný za to, že podá na iného občana na úrad alebo na zamestnávateľa sťažnosť, žalobu alebo návrh na začatie trestného stíhania.

Ak sa porušenia týchto práv dopustí úrad práce, sociálnych vecí a rodiny, tak má občan právo podať úradu sťažnosť, pričom je úrad povinný na sťažnosť občana bez zbytočného odkladu odpovedať, vykonať nápravu, upustiť od takého konania a odstrániť jeho následky, pričom nesmie občana postihovať alebo znevýhodňovať preto, že si uplatňuje svoje práva vyplývajúce z práva na prístup k zamestnaniu.

Zákonným vyjadrením práva na slobodnú voľbu povolania (čl. 35 Ústavy Slovenskej republiky) v kombinácii s právo m na prácu je v § 14 ods. 7 zakotvené právo občanov slobodne si zvoliť

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zamestnanie a vykonávať ho na celom území Slovenskej republiky alebo možnosť si ho zabezpečiť v zahraničí.

4.2 UCHÁDZAČ O ZAMESTNANIE A OCHRANA OSOBNÝCH ÚDAJOV

4.2.1 Uchádzač o zamestnanie v zmysle zákona o službách zamestnanosti

Uchádzača o zamestnanie definuje zákon o službách zamestnanosti v § 6, v zmysle ktorého je ním občan, ktorý môže pracovať, chce pracovať, hľadá si zamestnanie a je vedený v evidencii uchádzačov o zamestnanie úradu a ktorý:

a) nie je zamestnanec,

b) nie je v pracovnoprávnom vzťahu na základe dohody o práci vykonávanej mimo pracovného pomeru alebo nevykonáva zárobkovú činnosť na základe právneho vzťahu podľa osobitného predpisu, ak v § 6 odsek 2 nie je ustanovené inak,

c) neprevádzkuje alebo nevykonáva samostatnú zárobkovú činnosť,

d) nevykonáva zárobkovú činnosť v členskom štáte Európskej únie alebo v cudzine.

Zákon o službách napriek uvedenému pripúšťa aj niektoré výnimky z uvedených ustanovení, ktoré spočívajú v tom, že uchádzač o zamestnanie môže:

a) byť v pracovnoprávnom vzťahu (avšak nesmie byť súčasne vo viacerých pracovnoprávnych vzťahoch) na základe dohody o práci vykonávanej mimo pracovného pomeru, ak trvanie tohto pracovnoprávneho vzťahu nepresiahne v úhrne 40 dní v kalendárnom roku a ak mesačná odmena nepresiahne v úhrne sumu životného minima pre jednu plnoletú fyzickú osobu podľa osobitného predpisu platnú k prvému dňu kalendárneho mesiaca, za ktorý sa preukazuje výška odmeny, u zamestnávateľa:

   – u ktorého bezprostredne pred zaradením do evidencie uchádzačov o zamestnanie nebol v pracovnom pomere alebo v obdobnom pracovnom vzťahu,

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

– ktorý ho v predchádzajúcich šiestich mesiacoch pred uzatvorením tohto pracovnoprávneho vzťahu neodmietol prijať do zamestnania sprostredkovaného úradom;

b) vykonávať osobnú asistenciu podľa osobitného predpisu, ak mesačná odmena nepresiahne v úhrne sumu životného minima pre jednu plnoletú fyzickú osobu podľa osobitného predpisu platnú k prvému dňu kalendárneho mesiaca, za ktorý sa preukazuje výška odmeny,

c) poskytovať údaje pre štatistiku rodinných účtov, ktorú vykonáva Štatistický úrad Slovenskej republiky, na základe dohody o práci vykonávanej mimo pracovného pomeru,

d) vykonávať dobrovoľnú vojenskú prípravu podľa osobitného predpisu, alebo

e) byť zaradený do aktívnych záloh, vykonávať pravidelné cvičenie alebo plniť úlohy ozbrojených síl Slovenskej republiky počas zaradenia do aktívnych záloh podľa osobitného predpisu.

4.2.2 Záujemca o zamestnanie

Na rozdiel od uchádzača je v zmysle § 7 zákona o službách zamestnanosti záujemcom o zamestnanie občan, ktorý si hľadá iné zamestnanie alebo ktorý má záujem o poskytovanie informačných a poradenských služieb a odborných poradenských služieb a nie je uchádzačom o zamestnanie.

4.2.3 Znevýhodnený uchádzač o zamestnanie

Osobitnou kategóriou sú tzv. znevýhodnení uchádzači o zamestnanie, pri ktorých berie právna úprava na zreteľ ich oslabenú pozíciu na trhu práce predovšetkým spočívajúcu užších možnostiach zamestnania sa. Na tieto účely je znevýhodneným uchádzačom o zamestnanie:

a) občan mladší ako 26 rokov veku, ktorý ukončil príslušným stupňom vzdelania sústavnú prípravu na povolanie v dennej forme štúdia pred menej ako dvomi rokmi a od jej ukončenia nemal pravidelne platené zamestnanie („absolvent školy“),

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

b) občan starší ako 50 rokov veku,

c) občan vedený v evidencii uchádzačov o zamestnanie najmenej 12 po sebe nasledujúcich mesiacov (ďalej len „dlhodobo nezamestnaný občan“),

d) občan, ktorý dosiahol vzdelanie nižšie ako stredné odborné vzdelanie podľa osobitného predpisu,

e) občan, ktorý najmenej 12 po sebe nasledujúcich kalendárnych mesiacov pred zaradením do evidencie uchádzačov o zamestnanie nemal pravidelne platené zamestnanie (zamestnanie, ktoré trvalo najmenej šesť po sebe nasledujúcich mesiacov),

f) štátny príslušník tretej krajiny, ktorému bol udelený azyl alebo ktorému bola poskytnutá doplnková ochrana,

g) občan, ktorý žije ako osamelá dospelá osoba s jednou alebo viacerými osobami odkázanými na jeho starostlivosť alebo starajúca sa aspoň o jedno dieťa pred skončením povinnej školskej dochádzky,

h) občan so zdravotným postihnutím.

4.3 UCHÁDZAČ O ZAMESTNANIE A PREDZMLUVNÉ PRACOVNOPRÁVNE VZŤAHY

Zákonník práce v ust. § 41 ukladá určité povinnosti budúcim účastníkom pracovného pomeru ešte pred uzatvorením pracovnej zmluvy, t.j. pred založením pracovného pomeru. Ide o povinnosti v rámci predzmluvných vzťahov, ktoré treba považovať za pracovnoprávne vzťahy. Predzmluvné vzťahy podľa § 41 Zákonníka práce v nadväznosti na § 1 Zákonníka práce sú výnimkou zo zásady, že pracovnoprávne vzťahy vznikajú najskôr od uzatvorenia pracovnej zmluvy (pozri dikciu § 1 Zákonníka práce „pokiaľ zákon neustanovuje inak“).

Na predzmluvné vzťahy sa vzťahuje antidiskriminačné právo, zákon 365/2004 Z.z. Podstatu predzmluvných vzťahov, ako sú upravené v § 41 Zákonníka práce, tvoria informačné povinnosti zamestnávateľa voči osobe uchádzajúcej sa o založenie pracovného pomeru, ako aj informačné povinnosti budúceho zamestnanca. A. Informačné povinnosti zamestnávateľa

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Povinnosť budúceho zamestnávateľa ešte pred uzatvorením pracovnej zmluvy, oboznámiť fyzickú osobu s právami a povinnosťami, ktoré pre ňu vyplynú z pracovnej zmluvy, je koncipovaná relatívne široko a sčasti zahŕňa aj povinnosť zamestnávateľa oboznámiť fyzickú osobu s pracovnými a mzdovými podmienkami. Súčasne je zamestnávateľ povinný oboznámiť budúceho zamestnanca s právnymi predpismi na zaistenie bezpečnosti a ochrany zdravia pri práci, ktoré musí zamestnanec pri svojej práci dodržiavať a s ustanoveniami upravujúcimi zákaz diskriminácie.

Podľa § 41 ods. 2 a 3 Zákonníka práce, ak sa na výkon práce vyžaduje zdravotná spôsobilosť alebo psychická spôsobilosť na prácu alebo iný predpoklad podľa osobitných predpisov, zamestnávateľ môže uzatvoriť pracovnú zmluvu len s fyzickou osobou zdravotne spôsobilou a psychicky spôsobilou na túto prácu, ktorá spĺňa uvedený predpoklad. Obdobné právne obmedzenie pre zamestnávateľa platí aj v prípade, že zamestnávateľ hodlá uzatvoriť pracovnú zmluvu s mladistvým zamestnancom.

Použitie termínu „zamestnávateľ môže“ uzatvoriť pracovnú zmluvu treba vykladať v právnom význame, „je oprávnený“, „smie“. Ide o obmedzenie zmluvnej voľnosti na strane zamestnávateľa, ktoré sa vzťahuje len na taký druh konkrétnej práce, pri výkone ktorej sa vyžaduje zdravotná spôsobilosť alebo psychická spôsobilosť podľa osobitných predpisov. V prípade, že by išlo o práce, pri výkone ktorých by sa nevyžadovala podľa osobitného predpisu osobitná zdravotná spôsobilosť alebo psychická spôsobilosť alebo iný predpoklad, resp. takýto osobitný predpis by neexistoval, zamestnávateľ by nebol oprávnený vyžadovať informácie o zdravotnom stave fyzickej osoby uchádzajúcej sa o prácu. Uzatvorenie pracovnej zmluvy bez ohľadu na potrebnú zdravotnú spôsobilosť zamestnanca treba zo strany zamestnávateľa posudzovať ako porušenie kogentných ustanovení zákona s možnosťou sankčných postihov najmä zo strany inšpekcie práce.

Zamestnávateľ má povinnosti aj voči zákonným zástupcom mladistvých zamestnancov. Je povinný ešte pred uzatvorením pracovnej zmluvy si vyžiadať vyjadrenie zákonného zástupcu mladistvého zamestnanca. Vyjadrenie zákonného zástupcu pred uzatvorením pracovnej zmluvy s mladistvým zamestnancom je podľa ZP dôležité z hľadiska záujmu samotného mladistvého zamestnanca. Jeho nedostatok nemá však vplyv na platnosť právneho úkonu s

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

výnimkou ustanovenia § 53 Zákonníka práce ods. 1, podľa ktorého zmluva o budúcej pracovnej zmluve medzi žiakom strednej odbornej školy alebo odborného učilišťa a zamestnávateľom sa pod sankciou neplatnosti môže uzavrieť len s predchádzajúcim súhlasom zákonného zástupcu žiaka.

4.3.1 Zákaz zamestnávateľa vyžadovať určité informácie

Okrem všeobecného právneho vymedzenia práva zamestnávateľa na informácie v rámci predzmluvných vzťahov Zákonník práce taxatívnym spôsobom vymedzuje okruh informácií, ktoré zamestnávateľ nesmie od zamestnanca vyžadovať v rámci predzmluvných vzťahov.

Podľa ustanovenia § 41 ods. 6 Zákonníka práce zamestnávateľ nesmie vyžadovať od fyzickej osoby informácie:

a) o tehotenstve,

b) o rodinných pomeroch,

c) o bezúhonnosti, s výnimkou ak ide o prácu, pri ktorej sa podľa osobitného

d) predpisu vyžaduje bezúhonnosť,

e) o politickej, odborovej a náboženskej príslušnosti.

Zákon č. 5/2004 Z.z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov rozširuje zákaz smerovaný voči zamestnávateľom v rámci predzmluvných vzťahov. Podľa § 62 ods. 3 citovaného zákona zamestnávateľ nesmie pri výbere zamestnanca vyžadovať informácie nielen o sexuálnej orientácii uchádzača o zamestnanie, ale ani žiadne iné informácie, ktoré odporujú dobrým mravom.

Zákon o službách zamestnanosti s účinnosťou od 1. mája 2018 ukladá zamestnávateľovi v ponuke zamestnania uviesť aj sumu základnej zložky mzdy, ktorú poskytne fyzickej osobe v prípade, ak ju prijme do pracovného pomeru. Zákon súčasne zakazuje zamestnávateľom zverejňovať ponuky zamestnania, ktoré obsahujú akékoľvek obmedzenie a diskrimináciu. Týmto spôsobom chcel zákonodarca v rámci predzmluvných vzťahov zvýrazniť ochranu najmä

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

osobných údajov a osobnostných práv fyzickej osoby uchádzajúcej sa o založenie pracovnoprávneho vzťahu.

Zákaz vyžadovať informácie o bezúhonnosti zamestnanca neplatí v prípadoch, ak ide o prácu, pri ktorej sa podľa osobitného predpisu vyžaduje bezúhonnosť zamestnanca alebo ak to vyžaduje povaha práce, ktorú má zamestnanec v pracovnom pomere vykonávať. Dokladom o bezúhonnosti zamestnanca je výpis, resp. odpis z registra trestov. Pod zákaz vyžadovať konkrétny druh informácií patria aj informácie zamestnávateľa na politickú, odborovú a náboženskú príslušnosť.

4.3.2 Informačné povinnosti fyzickej osoby – budúceho zamestnanca

Jedna časť informačných povinností sa viaže na informácie o skutočnostiach, ktoré bránia výkonu práce a druhá časť informácií sa viaže na informácie, ktoré by mohli zamestnávateľovi spôsobiť ujmu. Informácie, ktoré bránia výkonu práce mal zákonodarca, pokiaľ ide o budúci pracovný pomer, uviesť podmieňovacím spôsobom, t.j. malo ísť o informácie, ktoré by bránili výkonu práce napríklad zo zdravotného dôvodu. Preto medzi ne možno zaradiť najmä informácie o zdravotnom stave zamestnanca napríklad v prípade, že zamestnávateľ prijíma zamestnanca na rizikovú prácu.

Informácie, ktoré by mohli zamestnávateľovi spôsobiť ujmu, nie sú v Zákonníku práce konkretizované. Ide napríklad o informácie budúceho zamestnanca týkajúce sa výkonu konkurenčnej činnosti v prospech iného zamestnávateľského subjektu.

Zákonník práce ukladá fyzickej osobe – potenciálnemu zamestnancovi, ktorý je mladistvý, aj povinnosť informovať svojho budúceho zamestnávateľa o dĺžke pracovného času u iného zamestnávateľa. Táto právna povinnosť má veľký význam v nadväznosti na ustanovenie § 85 Zákonníka práce, ktorý zakotvuje pre mladistvého zamestnanca maximálny týždenný pracovný čas na 30 hodín, ak je mladistvý mladší ako 16 rokov, na 37 a pol hodiny v prípade, že je mladistvý starší ako 16 rokov. Uvedená zákonná hranica maximálneho týždenného pracovného času platí aj v prípade, ak by mladistvý pracoval pre viacerých zamestnávateľov. Zamestnávateľ, ktorý angažuje mladistvú fyzickú osobu do pracovného pomeru ešte pred

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

uzatvorením pracovnej zmluvy, musí vedieť o existujúcom rozsahu pracovného úväzku potenciálneho zamestnanca u iného zamestnávateľa.

Ak predzmluvné právne povinnosti poruší zamestnávateľ, podľa ustanovenia § 41 ods. 9 Zákonníka práce uchádzač o zamestnanie ho môže žalovať na príslušnom súde. Za predpokladu, že by preukázal vyžadovanie informácií nad rámec ustanovenia § 41 ods. 5, 6 a 8 Zákonníka práce, prislúcha mu podľa ods. 9 citovaného ustanovenia primeraná peňažná náhrada. V prípade sporu by išlo o pracovný spor vyplývajúci z pracovnoprávnych vzťahov, aj keď k uzatvoreniu pracovnej zmluvy ešte nedošlo.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

5 NEZÁKONNÉ ZÁSAHY DO OCHRANY SÚKROMIA ZAMESTNANCOV

S postupným rozvojom informačno-komunikačných prostriedkov a zavádzaním digitalizácie a internetizácie do výrobných a pracovných procesov vzniklo široké spektrum spôsobov monitorovania zamestnancov. Mnohé z týchto spôsobov monitorovania zamestnancov sú založené na pokročilých digitálnych technológiách, ktoré je v aplikačnej praxi veľmi často zástupcami zamestnancov alebo orgánom inšpekcie práce ťažko odhaliť. Preto sa nové formy a spôsoby monitorovania zamestnancov vykazujú vysokú latentnosť z hľadiska ich odhalenia. Novým fenoménom je monitorovanie zamestnancov prostredníctvom digitálnych aplikácií alebo prostredníctvom umelej inteligencie. V tejto časti našej vedeckej analýzy poukážeme na tradičné a nové spôsoby monitorovania zamestnancov pri výkone ich práce, pričom jednotlivé formy a spôsoby monitorovania zamestnancov sa môžu uskutočniť v každej fáze pracovnoprávneho vzťahu rôznymi subjektmi.

5.1 MONITOROVANIE PRED A PO SKONČENÍ PRACOVNOPRÁVNEHO VZŤAHU

Monitorovanie zamestnancov sa môže uskutočniť v každej fáze pracovnoprávneho vzťahu. Monitorovanie zamestnancov sa môžu uskutočniť v predzmluvných pracovnoprávnych vzťahoch, počas pracovnoprávneho vzťahu, ako aj počas výpovednej doby a po skončení pracovnoprávneho vzťahu.

V aplikačnej praxi veľmi často dochádza k monitorovaniu zamestnancov v rámci predzmluvných pracovnoprávnych vzťahoch. Personálne agentúry a personálne oddelenia zamestnávateľov častokrát vyhľadávajú informácie týkajúce sa uchádzačov o zamestnanie prostredníctvom internetových sociálnych sietí. Pokiaľ uchádzač o zamestnanie dobrovoľne na sociálnej sieti zdieľa svoje obrazové, zvukové alebo obrazovo-zvukové záznamy, k neoprávnenému zásahu do ochrany práva na súkromie uchádzača o zamestnanie nedôjde, pokiaľ zamestnávateľ prehliadku týchto digitálnych záznamov vyhodnotí vyložene len pre svoje účely potencionálneho zamestnania uchádzača o zamestnanie. Aplikačným problémom je, že na účely získania informácií týkajúcich sa uchádzača o zamestnanie sa vytvárajú rôzne profily, ktoré majú za cieľ „požiadať o kamarátstvo“ cez sociálne siete za účelom odokrytia potencionálne využiteľných informácií ohľadom dotvorenia osobného profilu uchádzača

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

o zamestnanie. V predzmluvných vzťahoch môže dochádzať k neoprávnenému monitorovaniu zamestnanca aj počas procesu výberového konania. Známe sú praktiky najmä rôznych nadnárodných veľkých korporácií, ktoré v rámci výberových procesov vystavujú uchádzačov o zamestnanie rôznym stresovým a iným zdanlivo nepredvídateľným situáciám, pri ktorých prítomní alebo externí experti spolupracujúci so zamestnávateľom vyhodnocujú intelektuálnu a behaviórnu stránku uchádzača o zamestnanie, a to všetko bez vedomia uchádzača o zamestnanie. V aplikačnej praxi sa využívajú aj situácie, kedy správne odpovede zaznamenané písomne uchádzačom o zamestnanie sa dávajú skúmať grafológom za účelom zistenia osobnostných predpokladov pre danú pracovnú pozíciu. Rovnako tak členmi výberových komisií častokrát bývajú rôzni experti z oblasti psychológie, odborníci z oblasti verbálnej a neverbálnej komunikácie, ktorí sa zameriavajú na iné ako vedomostné stránky uchádzača o zamestnanie. Aplikačným problémom však je, že o takéto skúmanie a monitorovanie uchádzačov o zamestnanie sa častokrát deje bez vedomosti a súhlasu uchádzača o zamestnanie.

Počas trvania pracovnoprávneho vzťahu môže dochádzať k neoprávnenému monitorovaniu zamestnancov, pričom ZP najväčšie práva prislúcha zamestnancovi počas trvania pracovnoprávneho vzťahu. Pred uzatvorením pracovnoprávneho vzťahu a po je skončení ZP nemá špeciálne ustanovenia, ktoré by regulovali ochranu súkromia fyzických osôb v právnom postavení uchádzačov o zamestnanie alebo bývalých zamestnancov. Takéto fyzické osoby musia využiť aplikáciu ustanovení § 11 a nasl. OZ upravujúcich ochranu súkromia fyzických osôb.

Po skončení pracovného pomeru najčastejšie dochádza k *tzv. právnemu monitorovaniu* bývalých zamestnancov, ktorí mali so zamestnávateľom uzatvorené konkurenčné doložky podľa§ 83a ZP. Počas obdobia, v rámci ktorého sa zaviazali, že po skončení pracovného pomeru, max. 1 rok po jeho skončení, nebudú vykonávať zárobkovú činnosť, ktorá mala k činnosti bývalého zamestnávateľa konkurenčný charakter, môže zo strany bývalého zamestnávateľa dochádzať k právnemu monitorovaniu tohto zamestnanca. Právne monitorovanie nevykonávania jeho zárobkovej činnosti nie je zásahom do súkromia bývalého zamestnanca, pokiaľ sa uskutočňuje z verejne dostupných zdrojov, ako napríklad lustráciou

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

v obchodnom registri alebo živnostenskom registri, poprípade v registri občianskych združení a pod. Pokiaľ však takéto monitorovanie uskutočňuje tretia osoba, najčastejšie v podobe súkromných detektívnych kancelárií, v aplikačnej praxi môže dochádzať ku skrytému faktickému preverovaniu takýchto skutočností, najmä v podobe utajeného mystery shoppingu, kedy tretia osoba v postavení zákazníka sa dopytuje o bývalého zamestnanca, či je neposkytne služby, ktoré poskytoval v pracovnom pomere k bývalému zamestnávateľovi, pričom výsledok bude oznámený bývalému zamestnávateľovi zamestnanca. Je nepochybné, že aj takýmto spôsobom môže dôjsť k narušeniu súkromia bývalého zamestnanca zo strany jeho zamestnávateľa po skončení pracovného pomeru, z ktorého však ešte maximálne rok po jeho skončení môžu vyplývať vzájomné práva a povinnosti v zmysle § 83a ZP.

5.2 SUBJEKTY MONITORUJÚCE ZAMESTNANCOV

Podľa teórie pracovného práva v pracovnom pomere medzi zamestnávateľom a zamestnancom je oprávnený na výkon kontroly práce zamestnanca v zásade zamestnávateľ a nie cudzí subjekt v externom prostrední mimo zamestnávateľa.[162] Z hľadiska subjektu, ktorý môže v aplikačnej praxi zamestnanca monitorovať, môžeme monitorovanie zamestnancov deliť na také, ktoré realizuje sám zamestnávateľ alebo tretia osoba. Treťou osobou môže byť najčastejšie subjekt poverený zamestnávateľom, ako napríklad súkromná bezpečnostná služba, súkromná detektívna kancelária alebo prevádzkovateľ monitorovacieho zariadenia. V širšom chápaní monitorovania zamestnancov to môže byť poverený príslušník PZ SR pri dodržiavaní pravidiel premávky na pozemných komunikáciách alebo prevádzky na železničných tratiach, inšpektor práce pri výkone inšpekcie práce, klient ako zákazník zamestnávateľa alebo autonómny systém umelej inteligencie, ktorý sám nezávisle od vôle zamestnávateľa dokáže vyhodnotiť výkonnosť zamestnanca na základe toho, že monitoruje jeho výkonnosť.

Súkromná bezpečnostná služba alebo detektívna služba býva využívaná v situáciách, kedy na základe vnútorného predpisu zamestnávateľa dochádza k obmedzovaniu súkromného života na pracovisku zamestnávateľa. Typickým príkladom sú rôzne interné predpisy v rámci

162 BARANCOVÁ, H.: Nové technológie v pracovnom práve a ochrana zamestnanca (možnosti a riziká). Praha: Leges, 2016, str. 54, ISBN: 978-80-7502-176-2.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

firemných kultúr zamestnávateľov, ktoré rôznym spôsobom obmedzujú partnerské alebo manželské spolužitie dvoch zamestnancov na rovnakom pracovisku. Práve za účelom preverenia týchto skutočností bývajú často využívané uvedené spoločnosti. V niektorých prípadoch sú takéto spoločnosti poverované na preverenie skutočností týkajúcich sa prekážok v práci na strane zamestnanca. Typickým príkladom je dodržiavanie liečebného režimu zamestnanca počas prvých desiatich dní jeho dočasnej pracovnej neschopnosti, prípadne možnosť využiť návštevu lekára mimo pracovného času zamestnanca.

Pokiaľ prevádzkovateľom externého zariadenia nainštalovaného na pracovisku zamestnávateľa je iný subjekt ako zamestnávateľ, tak tento subjekt spracováva a uchováva osobné údaje zamestnanca v rámci jeho monitorovania na pracovisku. V aplikačnej praxi sa jedná o prevádzkovateľov zabezpečovacích systémov založených na snímaní biometrických údajov zamestnancov alebo prevádzkovateľov personálnych systémov, ktoré o zamestnancovi zbierajú údaje v nich obsiahnuté, ktoré z hľadiska ich obsahu tvoria osobné údaje zamestnanca.

S postupnou digitalizáciou a automatizáciou pracovných postupov sa možno čoraz viac stretnúť s monitorovaním zamestnancov umelou inteligenciou, ktorá o zamestnancovi zaznamenáva všetky údaje pri výkone jeho práce. Môže zaznamenávať porušenia výrobných procesov, prestávky v práci, normy spotreby práce a pod. Aplikačným problémom takýchto systémov umelej inteligencie je, že zozbierané údaje vyhodnocuje autonómny systém umelej inteligencie, ktorý je pomerne do veľkej miery nezávislý od posudzovania zamestnávateľom a jeho zamestnancami, pričom je problematická pričítateľnosť výsledkov umelej inteligencie zamestnávateľovi. Takto zozbierané údaje sa mnohokrát vyhodnocujú bez bližšieho skúmania zavinenia zamestnanca a majú priamy vplyv na práva zamestnanca, ako napríklad nesplnenie interných kritérií pre odmeňovanie zamestnanca vo vyššej triede bez ohľadu na to, či zamestnanec zavinil alebo nezavinil dôvody, ktoré interný systém umelej inteligencie vyhodnotil ako nesplnenie kritérií pre zaradenie zamestnanca do vyššieho platovej triedy v rámci interného systému odmeňovania zamestnancov u zamestnávateľa.

5.3 MONITOROVANIE E-MAILOVEJ KOMUNIKÁCIE

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Prvou formou kontroly obsahu e-mailovej komunikácie je jej skenovanie, pričom skríning e-mailov sa uskutočňuje predovšetkým na účely detekcie vírusov, odfiltrovania spamu a detekcie vopred určeného obsahu. Pri skríningu elektronickej pošty poskytovatelia služieb elektronickej pošty musia zabezpečiť, aby obsah e-mailov a príloh zostal v tajnosti, s obsahom e-mailov sa nesmie oboznámiť žiadna osoba, a to ani zamestnávateľ. V prípade nájdenia vírusov musí byť nainštalovaný softvér, ktorý poskytuje dostatočné záruky, pokiaľ ide o zachovanie dôveryhodnosti korešpondencie.[163] S rozvojom nových technológii v oblasti softvérových produktov je možné zo strany zamestnávateľa z miesta jeho pracoviska sledovať, či došlo k otvoreniu e-mailov zamestnancom, ktorý vykonáva prácu z jeho domova, čím si zamestnávateľ nepriamo môže overiť, či počas vopred dohodnutého časového úseku zamestnanec vykonáva svoju prácu za predpokladu, že uvedený program na komunikáciu medzi zamestnávateľom a zamestnancom má zamestnanec nainštalovaný len na svojom jednom technickom zariadení. V súčasnej dobe je možné, aby v rámci služby „Did they read it“ zamestnávateľ bez možnosti a vedomosti zamestnanca zamestnávateľ zistil, či odoslaný e-mail bol zamestnancom prečítaný, koľkokrát si ho zamestnanec prečítal alebo či bol naopak poslaný tretím osobám. Aplikačným problémom však je, že táto služba sa uskutočňuje skrytou formou bez akejkoľvek vedomosti zamestnanca.164

Zároveň je potrebné povedať, že súkromná pošta na pracovnú e-mailovú adresu zamestnanca nepatrí, ak to výslovne zamestnávateľ zamestnancovi nepovolí. V prípade, ak na základe identifikačných znakov, ako sú odosielateľ, príjemca alebo na základe koncovky došlého e-mailu je zrejmé, že sa jedná o e-mail súkromný, zamestnávateľ ho nemôže otvoriť a prečítať. Ak na podklade týchto indikátorov nie je na prvý pohľad zrejmé, že sa jedná o súkromný e-mail zamestnanca a zamestnávateľ ho otvorí, je povinný ihneď ukončiť čítanie obsahu e-mailu.[165]

---

163 BARANCOVÁ, H. a kol.: Základné práva a slobody v pracovnom práce. Plzeň: Aleš Čeněk, 2012. 118 s., ISBN: 97-80-7380-422-0.

164 BARANCOVÁ, H.: Práva zamestnancov v Európskej únie. 1.vyd. Praha: Leges, 2016, 140 s., ISBN: 978-80-7502-117-5.

165 MORÁVEK, J.: Ochrana osobních údaju v pracovněprávních vztazích. 1. Vyd. Praha: Wolters Kluwer ČR, 2013., 436 s., ISBN: 978-80-7478-139-1.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Kontrola e-mailovej pošty zamestnanca je zo strany zamestnávateľa relatívne častá, zriedkakedy však oprávnená. Z rozsudku Európskeho súdu pre ľudské práva v právnej veci Barbulescu zo dňa 5. septembra 2017 vyplýva, že komunikácia zamestnanca na pracovisku prislúcha pod pojem súkromný život a ochrana korešpondencie.[166] V súvislosti s kontrolou elektronickej pošty je potrebné odlišovať súkromnú elektronickú poštu od pracovnej elektronickej pošty. Za súkromnú elektronickú poštu možno považovať aj odoslanie elektronickej pošty na pracovný e-mail druhého zamestnanca, ak jej obsah nijako nesúvisí s pracovnou činnosťou alebo činnosťou zamestnávateľa. V prípadoch, kedy zamestnávateľ umožní svojím zamestnancov využívanie pracovnej elektronickej pošty na súkromné účely, je potrebné zo strany zamestnávateľa dôsledne dodržiavať právo na ochranu súkromia zamestnanca a súkromnú elektronickú poštu zamestnanca neprečítať.[167] Ak na podklade týchto indikátorov nie je na prvý pohľad zrejmé, že sa jedná o súkromný e-mail zamestnanca a zamestnávateľ ho otvorí, je povinný ihneď ukončiť čítanie obsahu e-mailu.[168] V oblasti e-mailovej komunikácie dochádza k monitorovaniu zamestnancov prostredníctvom skríningu elektronickej pošty na účely odfiltrovania spamu, na účely detekcie vopred určeného obsahu alebo prostredníctvom nových druhov softvérových produktov sledujúcich, či došlo alebo nedošlo k otvoreniu e-mailu a pod.[169]

5.4 KONTROLA NA PRACOVISKU POMOCOU VIDEOKAMIER ALEBO MIKROFÓNOV

Kontrola a monitoring zamestnancov na pracovisku prostredníctvom videokamier a mikrofónov je prípustná len za predpokladu, že takýto spôsob monitorovania zamestnancov je v zásade jediným prostriedkom na dosiahnutie určitého, konkrétneho a legitímneho cieľa. Za takýto cieľ bude možné považovať v aplikačnej praxi opatrenie na zabránenie krádežiam v obchodnej prevádzke zamestnávateľa. Napríklad kontrola *tzv. čistého pracovného výkonu* zamestnancov podľa rakúskeho pracovného práva je v rozpore so zákonom ako aj Európskym

[166] HROMADA, M.: Ochrana osobnosti zaměstnance při elektronické komunikaci. str. 161. In: BARANCOVÁ, H., OLŠOVSKÁ, A. (eds.): Pracovné právo v digitálnej dobe. Praha: Leges, 2017, 304 s., ISBN: 978-80-7502-259-2.
[167] BARANCOVÁ, H.: Nové technológie v pracovnom práce a ochrana zamestnanca (možnosti a riziká). Praha: Leges, 2016, str. 40, ISBN: 978/80-7502-176-2.
[168] MORÁVEK, J.: Ochrana osobních údaju v pracovněprávních vztazích. 1. Vyd. Praha: Wolters Kluwer ČR, 2013., 436 s., ISBN: 978-80-7478-139-1.
[169] BARANCOVÁ, H.: Práva zamestnancov Európskej únie. Praha: Leges, 2016, str. 140, ISBN: 978-80-7502-117-5.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

dohovorom a Chartou, ak je uvedená kontrola systematická a nespĺňa podmienky náhodnej kontroly.[170] Veľký senát Európskeho súdu pre ľudské práva rozhodnutím López Ribalda a i. proti Španielsku zo dňa 17. 10. 2019 vyslovil, že monitorovanie zamestnancov supermarketu skrytými kamerami nie je porušením práva na rešpektovanie ich súkromného a rodinného života, garantovaného článkom 8 Európskeho dohovoru o ľudských právach. Ide o prelomové rozhodnutie aj z toho dôvodu, že veľký senát pomerom hlasov 14:3 zmenil predchádzajúce rozhodnutie tohto Súdu, ktoré vyslovilo opačný záver, a značne modifikuje aj aplikáciu niektorých princípov sformulovaných Súdom v rozhodnutí Bărbulescu proti Rumunsku. Veľmi častým aplikačným problémov je, že videokamery na pracovisku zamestnávateľa monitorujú priestory, ktoré z hľadiska ich určenia sú výlučne určené pre sociálne a biologické potreby zamestnancov. Typickým príkladom je priestor slúžiaci na regeneráciu zamestnancov, prebaľovacie kútiky pre dojčiace matky alebo zamestnancov starajúcich sa o svoje deti, priestory určené pre deti zamestnancov na pracovisku, priestory určené na fajčenie pred budovou zamestnávateľa v jeho areáli a pod.

5.5 KONTROLA PROSTREDNÍCTVOM BIOMETRICKÝCH ÚDAJOV

Biometrické údaje zamestnávatelia využívajú najmä na účely evidencie dochádzky do zamestnania. Definíciu biometrických údajov možno nájsť v zákone o ochrane osobných údajov. Podľa § 5 písm. c) zákona o ochrane osobných údajov sú biometrickým údajmi osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje. V zmysle § 16 ods. 1 zákona o ochrane osobných údajov sa zakazuje spracúvanie osobitných kategórií osobných údajov. Osobitnými kategóriami osobných údajov sú údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, ***biometrické údaje***, údaje týkajúce sa zdravia alebo údaje

[170] BARANCOVÁ, H.: Nové technológie v pracovnoprávnych vzťahoch. Praha: Leges, 2017, str. 114, ISBN: 978-80-7502-253-0.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby. Z uvedeného zákonného zákazu spracovania biometrických údajov existujú zákonné výnimky, a to napríklad:

a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov aspoň na jeden konkrétny účel; súhlas je neplatný, ak jeho poskytnutie vylučuje osobitný predpis;

b) spracúvanie je nevyhnutné na účel plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva, práva sociálneho zabezpečenia, sociálnej ochrany alebo verejného zdravotného poistenia podľa osobitného predpisu, medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo podľa kolektívnej zmluvy, ak poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby;

c) spracúvanie je nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby alebo inej fyzickej osoby, ak dotknutá osoba nie je fyzicky spôsobilá alebo právne spôsobilá vyjadriť svoj súhlas,

d) spracúvanie vykonáva v rámci oprávnenej činnosti občianske združenie, nadácia alebo nezisková organizácia poskytujúca všeobecne prospešné služby, politická strana alebo politické hnutie, odborová organizácia, štátom uznaná cirkev alebo náboženská spoločnosť a toto spracúvanie sa týka iba ich členov alebo tých fyzických osôb, ktoré sú s nimi vzhľadom na ich ciele v pravidelnom styku, osobné údaje slúžia výlučne pre ich vnútornú potrebu a nebudú poskytnuté príjemcovi bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby.

K problematike súhlasu zamestnanca k udeleniu súhlasu s monitorovaním prostredníctvom biometrických údajov uvádzame rozhodnutie Najvyššieho správneho sudu Poľskej republiky, podľa ktorého využitie biometrických údajov na kontrolu evidencie dochádzky zamestnancov do práce je neprimerané. Súčasne tento súd uviedol, že pri chýbajúcej rovnosti účastníkov

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

pracovnoprávneho vzťahu nie je možné hovoriť o dobrovoľnom súhlase zamestnanca so spracovaním biometrických údajov.[171]

K problematike využívania biometrických údajov sa taktiež vyjadril Úrad na ochranu osobných údajov, podľa ktorého: „spracúvanie osobných údajov **v tzv. biometrickom informačnom systéme na účel evidencie pracovnej dochádzky nie je nevyhnutné ani primerané.** Predmetný účel spracúvania (evidencia pracovnej dochádzky) je možné rovnako efektívne dosiahnuť využitím príp. vhodným kombinovaním iných ako biometrických prostriedkov spracúvania osobných údajov, ktoré sú menej rizikové z hľadiska neoprávnených zásahov do základného ľudského práva na ochranu súkromia a osobných údajov. Vedenie evidencie pracovnej dochádzky je možné charakterizovať ako štandardné spracúvanie osobných údajov, ktoré je možné bez neprimerane zvýšeného úsilia a nákladov rovnako efektívne dosiahnuť efektívnym využívaním menej invazívnych a rizikových prostriedkov spracúvania ako je samotné využitie biometrickej technológie (napr. o rôzne softvérové aplikácie, kamerové systémy, RFID karty a ich kombinovanie). Z uvedeného vyplýva, že spracúvaním biometrických údajov zamestnancov navrhovateľa na účel evidencie pracovnej dochádzky v rámci predmetných podmienok spracúvania osobných údajov nie je v súlade s § 13 ods. 5 zákona č. 122/2013 Z. z., takže nie je možné akceptovať navrhovateľovo tvrdenie, že daný spôsob spracúvania biometrických údajov nijako neporušuje zákon č. 122/2013 Z. z. a je nevyhnutný na dosiahnutie zamýšľaného účelu, a to riadnej a spoľahlivej dochádzky zamestnancov do zamestnania. Faktor možného zvýšenia produktivity práce a optimalizácie nákladov spočívajúci v zavedení biometrického dochádzkového systému je diskutabilný a s určitosťou neprevyšuje záujem na ochrane základného ľudského práva na ochranu súkromia a osobných údajov navrhovateľových zamestnancov.“ Výsledkom tak je, že mnoho firiem má inštalované reálne biometrické systémy určené na kontrolu zamestnancov, ktoré sú spracúvané jednak bez právneho základu a jednak bez osobitnej „okrúhlou pečiatkou Úradu“ posvätenej registrácie, čo vedie k závažnému porušeniu účinného Zákona o ochrane osobných údajov.[172]

[171] Rozhodnutie Najvyššieho správneho súdu Poľskej republiky sp. zn.: I OSK 249/09.
[172] ZIMEN, O.: Biometrické dochádzkové systémy a ich problémy s reguláciou ochrany osobných údajov. Dostupné na: https://www.pravnenoviny.sk/biometricke-dochadzkove-systemy-a-ich-problemy-s-regulaciou-ochrany-osobnych-udajov. (Navštívené dňa 27.10.2023, 18:50 hod.)

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Používanie biometrických údajov a osobitne rozpoznávanie tvárí predstavuje zvýšené riziká pre práva dotknutých osôb. Je veľmi dôležité, aby sa pri používaní takýchto technológií dôsledne dodržiavali zásady zákonnosti, nevyhnutnosti, primeranosti a minimalizácie údajov, ako je stanovené vo všeobecnom nariadení o ochrane údajov. Zatiaľ čo používanie týchto technológií možno vnímať ako obzvlášť účinné, prevádzkovatelia by mali najprv posúdiť vplyv na základné práva a slobody a zvážiť menej rušivé prostriedky na dosiahnutie svojho oprávneného účelu spracúvania.

Na to aby mohlo ísť o spracúvanie osobitných kategórií osobných údajov, musí byť splnená podmienka, že biometrické údaje sa spracúvajú *„na jedinečnú identifikáciu fyzickej osoby“.* V aplikačnej praxi sa musia zohľadniť tri kritériá:

a) povaha údajov: údaje týkajúce sa fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby;

b) prostriedky a spôsob spracúvania: údaje, ktoré sú *„výsledkom osobitného technického spracúvania“*;

c) účel spracúvania: údaje musia byť použité na účel jedinečnej identifikácie fyzickej osoby.

Monitorovanie zamestnancov prostredníctvom ich biometrických údajov veľmi často býva využívaní pri vstupoch do budov zamestnávateľmi, prípadne do vyhradených priestorov zamestnávateľa s údajmi, s ktorými sa môžu oboznámiť len niektorí zamestnanci zamestnávateľa, ktorí prešli *tzv. bezpečnostnou previerkou* alebo špeciálnym interným oprávnením alebo povolením zamestnávateľa.

Takýto spôsob prístupu môže zamestnávateľ využívať, len aj dotknutí zamestnanci vopred poskytli výslovný informovaný súhlas v súlade s článkom 9 ods. 2 písm. a) Nariadenia GDPR. Aby sa zabezpečilo, že nebude zachytený iný zamestnanec, ktorý predtým neposkytol súhlas, metódu rozpoznávania tvárí musí dotknutý zamestnanec aktivovať sám, napríklad stlačením tlačidla. Na zaistenie zákonnosti spracúvania musí zamestnávateľ ponúkať náhradný spôsob prístupu do budovy alebo priestoru zamestnávateľa bez spracúvania biometrických údajov, napr. pomocou preukazov alebo kľúčov. Môže to byť z dôvodu výpadku systémov spracovania

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

biometrických údajov alebo z dôvodu zdravotného handicapu niektorých zamestnancov zamestnávateľa.

V súlade so zásadou minimalizácie údajov musia zamestnávatelia zabezpečiť, aby údaje získané z digitálnej snímky na účely vyhotovenia vzoru neboli neprimerané a obsahovali len informácie požadované na konkrétny účel, čím sa predíde možnému ďalšiemu spracúvaniu. Mali by sa zaviesť opatrenia, ktoré zaistia, že sa vzory nebudú môcť prenášať medzi biometrickými systémami. Na identifikáciu a jej potvrdenia a overenia sa bude vyžadovať ukladanie vzorov na neskoršie porovnávanie. Zamestnávatelia musia zabezpečiť bezpečné úložisko takýchto údajov. Získané biometrické údaje by sa mali ukladať len v zariadeniach vo vlastníctve alebo v držbe zamestnávateľa, aby sa predišlo k neoprávnenému odcudzeniu takýchto údajov zamestnancov. Pokiaľ je monitorovaných viacero priestorov zamestnávateľa, možno len odporučiť, aby sa každé jedno kontrolované miesto monitorovalo technickým zariadením na zber biometrických údajov samostatne, pričom všetky technické zariadenia by mala na starosti poverená osoba zamestnávateľa a biometrické údaje na úložiská by mali ukladať v zašifrovanej podobe alebo pod bezpečnostnými kľúčmi. V aplikačnej praxi sa možno stretnúť najmä s algoritmickými prvkami. Po skončení pracovného pomeru zamestnancov musí zamestnávateľa zabezpečiť, aby sa zozbierané biometrické údaje predpísaným spôsobom vymazali. Takúto potrebu využívania biometrických údajov o zamestnancovi je potrebné skúmať vždy, keď nastane právna alebo faktická skutočnosť, ktorá už neodôvodňuje používanie biometrických údajov o zamestnancovi. Typickým príkladom je zmena pracovných podmienok zamestnanca pri zmene pracovnej pozície, na základe ktorej už zamestnávateľ nepotrebuje využívanie biometrických údajov zamestnanca, nakoľko na danej pracovnej pozícií sa už nepotrebuje napríklad vstupovať do kontrolovaných priestorov zamestnávateľa, do ktorých je možný vstup na základe zosnímania biometrických údajov zamestnanca.

5.6 MYSTERRY SHOPPING

Mysterry shopping predstavuje ďalší inovatívny spôsob monitorovania zamestnancov zamestnávateľa. Mysterry shopping ako forma monitorovania zamestnancov na pracovisku zamestnávateľa sa čoraz viac stáva súčasťou firemnej kultúry a politiky čoraz väčšieho počtu zamestnávateľov. Súčasťou politiky zamestnávateľov v oblasti mysterry shoppingu sú rôzne

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

interné normatívne právne akty zamestnávateľov, ktoré rôznymi spôsobmi upravujú podmienky výkonu mysterry shoppingu na pracovisku zamestnávateľa. Samotné programy zamestnávateľov v oblasti mysterry shoppingu sa zameriavajú na legitímnosť a transparentnosť zozbieraných údajov a ich následné interné vyhodnotenie pre potreby zamestnávateľa s pracovnoprávnymi dôsledkami na zamestnancov.

Problematika výkonu kontroly prostredníctvom *mystery shoppingu* naráža na právne a etické problémy a dilemy. Medzi etické dilemy výkonu kontroly zamestnancov patrí vznik nedôvery zamestnávateľa voči zamestnancovi, na základe ktorého nariadi skrytú formu kontroly tohto zamestnanca. Súčasťou tejto etickej dilemy je morálne právo zamestnanca na to, že v priebehu svojho výkonu práce môže byť monitorovaný aj takouto skrytou formou. Výkon kontroly prostredníctvom mystery shoppingu naráža na viaceré právne problémy. Základnou otázkou pri výkone kontroly prostredníctvom mystery shoppingu je, či takéto monitorovanie zamestnancov musí spĺňať podmienky upravené v § 13 ods. 4 Zákonníka práce, najmä ak sa jedná o nepravidelné a skutočne náhodilé monitorovanie svojich zamestnancov. Podľa Barancovej pri jednorazovom výkone kontroly prostredníctvom mystery shoppingu nie je naplnená skutková podstata § 13 ods. 4 Zákonníka práce. Prikláňame sa k právnemu záveru, že pokiaľ chce zamestnávateľ nariadiť výkon kontroly svojich zamestnancov prostredníctvom tejto formy kontroly, nemusí dodržať ustanovenie § 13 ods. 4 Zákonníka práce, ak sa vzhľadom na intenzitu kontroly počas vymedzeného obdobia jedná o mimoriadnu a jednorázovú situáciu. Súčasne sme tohto názoru, že pokiaľ si zamestnávateľ splní podmienky uvedené v § 13 ods. 4 Zákonníka práce, nemusí vopred informovať zamestnancov, že konkrétny dátum bude takáto forma kontroly realizovaná. Postačuje, aby takáto kontrola prebehla v bližšie ohraničenom termíne na výkon kontroly. Je nutné dodať, že pri objednávke služby na monitorovanie svojich zamestnancov prostredníctvom *mystery shoppingu* ani samotný zamestnávateľ nemusí vedieť, kedy jeho zmluvný partner uskutoční takýto monitoring jeho zamestnancov.

S postupným rozvojom internetizácie a digitalizácie sa čoraz viac rozvíjajú možnosti, ako uskutočniť samotný výkon kontroly na základe prostredníctvom *mystery shoppingu*. Do úvahy prichádzajú viaceré formy jeho realizácie, ako napríklad výkon kontroly na pracovisku

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zamestnávateľa, prostredníctvom telefonického rozhovoru alebo prostredníctvom mailových dopytov na zamestnancov. Z výkonu kontroly sa vyhotovujú rôzne skryté audiovizuálne nahrávky alebo rôzne obrazové a obrazovo-zvukové snímky bez vedomia zamestnancov. Súčasťou výkonu kontroly prostredníctvom *mystery shoppingu* môžu byť viaceré aspekty výkonu práce zamestnanca na pracovisku. Predmetom monitorovania zamestnanca môže byť jeho ľudský prístup k zákazníkovi, čas trvania prístupu zamestnanca k zákazníkovi na obchodnej prevádzke, dodržiavanie predpisov zaisťujúcich bezpečnosť a ochranu zdravia pri práci alebo napríklad skúmanie zákazu konaní, ktoré sú predmetom regulácie správnych alebo trestných kódexov, ako napríklad skúmanie, či zamestnanec predá zákazníkovi tovar bez pokladničného dokladu alebo či príjme ponúknutý úplatok. K tejto problematike uvádzame, že skúmanie takýchto zakázaných konaní je predmetom regulácie správnych orgánov alebo orgánov činných v trestnom konaní. Účelom pracovného práva nie je v zásade skúmať, či sa zamestnanec pri výkone svojej práce dopúšťa alebo nedopúšťa trestnej činnosti. Na druhej strane uvádzame, či je v právnom a etickom záujme zamestnávateľa a jeho podnikateľskej činnosti, aby sa v jeho prevádzke a na jeho pracovisku zamestnanci nedopúšťali konaní, ktoré sú osobitnými právnymi predpismi zakázané a sankcionované v neprospech samotného zamestnanca alebo zamestnávateľa. Z uvedeného dôvodu sme toho názoru, že za týmto účelom je zamestnávateľ pri dodržaní podmienok oprávnený uskutočniť výkon kontroly svojich zamestnancov aj za takýmto účelom prostredníctvom *mystery shoppingu*.

Za problematické však považujeme, akými nástrojmi a spôsobmi osoba vykonávajúca výkon kontroly zamestnancov prostredníctvom *mystery shoppingu* dospeje k negatívnym záverom v neprospech konkrétneho zamestnanca. Sú známe prípady, kedy osoba vykonávajúca výkon kontroly zamestnancov prostredníctvom *mystery shoppingu* ponúkne zamestnancovi zamestnávateľa úplatok za určitú službu, prípadne na dosiahnutie záverov o zamestnancoch využívajú nátlak a rôzne formy provokácie, zinscenované krádeže v prevádzkach zamestnávateľov alebo zinscenované iné mimoriadne udalosti bez toho, aby sa jednalo o taktické a bezpečnostné cvičenia zamestnávateľa. Uvedené spôsoby výkonu kontroly prostredníctvom *mystery shoppingu* sú problematické najmä pri vyvodzovaní následnej pracovnoprávnej zodpovednosti voči zamestnancom.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Najvyšší súd Poľskej republiky sa vo svojom rozsudku z 15. novembra 2017 (III PK 161/16) vyslovil v podstate proti používaniu manipulačných metód zamestnávateľmi a takých, ktoré sú úmyselné alebo majú inštrumentálny účel, ako porušenie všeobecnej povinnosti lojality zamestnávateľa. k zamestnancom a právo zamestnancov pracovať v *„priateľskom prostredí“*. Opatrenia na kontrolu bezúhonnosti zamestnancov povolil Najvyšší súd Poľskej republiky len vo výnimočných prípadoch. Rozhodnutie sa týkalo toho, že zamestnanec dostal *„kontrolovaný úplatok“*; z pohľadu *mystery shoppera* však stojí za zmienku, že pracovné súdy vydávajú negatívne hodnotenia provokácie používané na odôvodnenie výpovede zamestnanca (podobné závery možno vyvodiť aj z rozsudku Okresného súdu v Gorzówe Wielkopolskom z 5. apríla 2018, VI Pa 85/17). To znamená, že zamestnávatelia by sa mali zásadne vyhýbať tomu, aby mystery shopper navádzal na úmyselné agresívne, kverulačné alebo iné neprimerané správanie, ktoré by mohlo vyvolať špecifickú reakciu zamestnancov, ktorá by bola dôvodom na prepustenie. Vyššie uvedený rozsudok a riedka judikatúra zaoberajúca sa *mystery shoppingom* (napr. rozsudok Krajského súdu v Lubline z 10. januára 2018, VIII Pa 155/17), obidva dokazujú, že pracovné súdy robia iné, pre zamestnancov priaznivejšie, hodnotenie tzv. správanie zamestnancov v situáciách, ktoré zinscenoval zamestnávateľ. Vo vyššie citovanom rozsudku Krajského súdu v Lubline sa odvolací súd stotožňuje s názorom prvostupňového súdu, že ***„pri hodnotení kvality a angažovanosti zamestnanca treba v prvom rade prihliadať na posúdenie kontaktov so skutočnými zákazníkmi“***. S ohľadom na vyššie uvedené by mali zamestnávatelia postupovať pri rozviazaní pracovného pomeru zamestnanca výlučne na základe jediného negatívneho hodnotenia *mystery shoppingu*.[173]

V aplikačnej praxi má výkon kontroly prostredníctvom mystery shoppingu pozitívne ako aj negatívne aspekty. Pokým pozitívne aspekty výkonu takejto skrytej formy kontroly sa prejavujú najmä v prospech zamestnávateľa podobe zvýšenej produkcie práce, tak na strane zamestnanca sa zväčša prejavujú negatívne aspekty výkonu takejto kontroly. Medzi

[173] MAGNUSKA, K.: A mystery shopper is not always useful in dismissing an employee. Dostupné na: https://hrlaw.pl/en/a-mystery-shopper-is-not-always-useful-in-dismissing-an-employee/. (Navštívené dňa 27.10.2023, 21:20 hod.)

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

najčastejšie negatívne aspekty výkonu takejto formy kontroly patrí zvýšenie stresu zamestnancov, rozšírenie nedôvery medzi zamestnancami zamestnávateľa alebo zvýšenie počtu absencií na pracovisku zamestnávateľa z dôvodu eliminácie podrobenia sa náhodnej skrytej kontrole.

5.7 NOVÉ TRENDY V OBLASTI MONITOROVANIA ZAMESTNANCOV

Prvým trendom v oblasti monitorovania zamestnancov sú nové softwérové programy. Existuje niekoľko typov počítačových monitorovacích systémov. Počítačový softvér môže napríklad kontrolovať presnosť výkonu zamestnancov a rýchlosť stláčania kláves, najmä pre tých, ktorí sa podieľajú na spracovaní textu a úlohách zadávania údajov. Pomocou terminálu na zobrazovanie videa (VDT) môžu zamestnávatelia sledovať počet chýb za hodinu, frekvenciu zdvihov pre každú úlohu, počet úloh, presnosť zadávaného textu a rýchlosť transakcií zamestnancov. Počítačové softvéry umožňujú zamestnávateľom viesť záznamy o výkone zamestnancov, poskytujú im informácie potrebné na stanovenie výkonnostných štandardov a pomáhajú im pri procese hodnotenia a odmeňovania zamestnancov.

Počítačové monitorovanie možno použiť aj na sledovanie množstva času, ktorý zamestnanci strávia mimo svojho počítača alebo rozsahu ich nečinnosti počas pracovného času. Nielenže tieto systémy umožňujú zamestnávateľom mať bližší prehľad o zamestnancoch, ale tiež poskytujú zamestnancom prístup k informáciám o ich vlastnom výkone, ktoré potom môžu využiť na zlepšenie.

Moderné počítačové systémy dokážu napríklad automaticky bez vedomia zamestnanca zaznamenať jeho mimopracovnú aktivitu na internete tým, že *screeningujú* otvorené prehliadače v jeho počítači, automaticky spúšťajú nahrávanie sledovaných videí na externých úložiskách, ako napríklad sledovanie filmov na Netflixe, alebo ukladajú dokumenty na externé úložisko s následnou filtráciou obsahu nesúvisiaceho s náplňou práce zamestnanca, ktoré si dal vytlačiť zamestnanec v práci na tlačiarni zamestnávateľa.

Druhým trendom pri monitorovaní zamestnancov je systém založený na *tzv. aktívnych odznakoch* zamestnancov. Monitorovanie zamestnancov prostredníctvom *tzv. aktívnych odznakoch (z ang. Badge system)* predstavuje aktuálny najmodernejší trend v oblasti

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

monitorovania zamestnancov. Tento spôsob monitorovania zamestnancov spočíva v tom, že zamestnanci pohybujúci sa po pracoviska zamestnávateľa majú na sebe pripnuté monitorovacie zariadenia na lokalizáciu ich pohybu na pracovisku za účelom zvýšenia efektivity práce a zníženia neefektívneho času stráveného neúspešnými pokusmi spojiť sa zo zamestnancami navzájom prostredníctvom e-mailov alebo telefonátov. Aj takýto systém monitorovania zamestnancov musí splniť podmienky uvedené v § 13 ods. 4 Zákonníka práce. Takýto systém monitorovania zamestnancov využíva internetové lokálne siete na pracoviskách zamestnávateľa. Tento systém využíva identifikačné karty zamestnancov, čítačky kariet a magnetické alebo elektronické zámky alebo body na pracovisku, ktoré musí zamestnanec pri výkone práce absolvovať.

Treťou novinkou v oblasti monitorovania zamestnancov je využitie umelej inteligencie pri výkone práce a jeho mimopracovných aktivít počas pracovnej doby, ktorá dokáže skúmať v priebehu času a priestoru mentálnu a zdravotnú stránku zamestnanca a vytvoriť o ňom behaviórny alebo zdravotný profil. Pokiaľ zamestnanec začne počas pracovnej doby alebo aj počas prestávky v práci tráviť viac času sledovaním webových stránok na internete zameraných na parciálnu časť zdravotného problému, moderné systémy umelej inteligencie dokážu automaticky predikovať, že zamestnanec začal mať zdravotné problémy súvisiace s konkrétnou časťou ľudského tela. Tieto systémy umelej inteligencie mnohokrát zachránia zamestnávateľov pred vznikom zodpovednosti zamestnávateľa za chorobu z povolania zamestnanca, pretože pokiaľ zamestnávateľ dostatočne jasne a skoro identifikuje možnú chorobu z povolania u zamestnanca a dostatočne skoro s ním skončí pracovný pomer, tým je väčšia pravdepodobnosť, že bude chýbať *kauzálny nexus* medzi výkonom jeho pôvodnej práce a aktuálnym vznikom zdravotného problému ako choroby z povolania, čím sa zamestnávateľ *de iure* vyhne vzniku zodpovednosti za vznik choroby z povolania. Obdobne to platí pre tehotných zamestnankyniach, ktoré začnú zamestnávateľovi nosiť potvrdenie o návšteve lekára od gynekológa a zvýšeným počtom navštívených webových stránok zameraných na tehotenstvo a materstvo, tak systémy umelej inteligencie dokážu takéto správanie vyhodnotiť pre zamestnávateľa ako rizikové a zamestnávateľ môže udeliť zamestnankyni výpoveď z pracovného pomeru alebo urobiť organizačnú zmenu s následkom skončenia jej pracovného

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

pomeru ešte pred tým, ako mu písomne oznámila, že je tehotná. Pri týchto systémoch však platí, že uvedené systémy umelej inteligencie sú výborným nástrojom na efektivitu a produkciu práce u zamestnávateľa, pokiaľ nedôjde k ich zneužitiu. Pokiaľ na základe takéhoto systému dokáže zamestnávateľ predikovať radikalizáciu zamestnanca pred vznikom bezpečnostného incidentu na pracovisku zamestnávateľa, uvedený systém umelej inteligencie potencionálne poslúžil na ochranu života a zdravia na pracovisku zamestnávateľa. Obdobne platí aj pri nutnosti zabezpečiť náhradného zamestnanca počas materskej a rodičovskej dovolenky za budúcu tehotnú zamestnankyňu. Pokiaľ však na základe takéhoto systému umelej inteligencie dôjde k vyvodeniu pracovnoprávnej zodpovednosti v podobe neoprávneného skončenia pracovného pomeru, sme toho názoru, že uvedené skončenie pracovného pomeru by malo byť zo strany všeobecných súdov vyhlásené za neplatné pre rozpor s § 13 ods. 4 Zákonníka práce a pre výkon práva v rozpore s dobrými mravmi.

5.7.1 Kontrola e-mailovej komunikácie zamestnanca

Prvou formou kontroly obsahu e-mailovej komunikácie je jej skenovanie, pričom skríning e-mailov sa uskutočňuje predovšetkým na účely detekcie vírusov, odfiltrovania spamu a detekcie vopred určeného obsahu. Pri skríningu elektronickej pošty poskytovatelia služieb elektronickej pošty musia zabezpečiť, aby obsah e-mailov a príloh zostal v tajnosti, s obsahom e-mailov sa nesmie oboznámiť žiadna osoba, a to ani zamestnávateľ. V prípade nájdenia vírusov musí byť nainštalovaný softvér, ktorý poskytuje dostatočné záruky, pokiaľ ide o zachovanie dôveryhodnosti korešpondencie.[174] S rozvojom nových technológii v oblasti softvérových produktov je možné zo strany zamestnávateľa z miesta jeho pracoviska sledovať, či došlo k otvoreniu e-mailov zamestnancom, ktorý vykonáva prácu z jeho domova, čím si zamestnávateľ nepriamo môže overiť, či počas vopred dohodnutého časového úseku zamestnanec vykonáva svoju prácu za predpokladu, že uvedený program na komunikáciu medzi zamestnávateľom a zamestnancom má zamestnanec nainštalovaný len na svojom jednom technickom zariadení. V súčasnej dobe je možné, aby v rámci služby *„Did they read it“* zamestnávateľ bez možnosti a vedomosti zamestnanca zamestnávateľ zistil, či odoslaný e-mail

[174] BARANCOVÁ, H. a kol.: Základné práva a slobody v pracovnom práce. Plzeň: Aleš Čeněk, 2012. 118 s., ISBN: 97-80-7380-422-0.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

bol zamestnancom prečítaný, koľkokrát si ho zamestnanec prečítal alebo či bol naopak poslaný tretím osobám. Aplikačným problémom však je, že táto služba sa uskutočňuje skrytou formou bez akejkoľvek vedomosti zamestnanca.[175]

Zároveň je potrebné povedať, že súkromná pošta na pracovnú e-mailovú adresu zamestnanca nepatrí, ak to výslovne zamestnávateľ zamestnancovi nepovolí. V prípade, ak na základe identifikačných znakov, ako sú odosielateľ, príjemca alebo na základe koncovky došlého e-mailu je zrejmé, že sa jedná o e-mail súkromný, zamestnávateľ ho nemôže otvoriť a prečítať. Ak na podklade týchto indikátorov nie je na prvý pohľad zrejmé, že sa jedná o súkromný e-mail zamestnanca a zamestnávateľ ho otvorí, je povinný ihneď ukončiť čítanie obsahu e-mailu.[176]

5.7.2 Monitorovanie internetových stránok a mobilných aplikácií

V súčasnej dobe je pomerne bežné, že zamestnanci využívajú svoj pracovný čas na iné ako na pracovné účely, pričom časť zo svojho pracovného času trávia prehľadávaním internetových stránok, ktoré nesúvisia s náplňou práce zamestnanca, alebo svoj pracovný čas trávia surfovaním na sociálnych sieťach. Z uvedeného dôvodu považujeme monitoring zamestnancov za legitímny záujem zamestnávateľa za účelom zistenia, či jeho zamestnanci skutočne využívajú pracovný čas na plnenie pracovných úloh. Ak sa rozhodne zamestnávateľ zaviesť sledovanie činnosti zamestnancov na internete, mal by uprednostniť také prostriedky a opatrenia, ktoré by primárne zamedzili alebo obmedzili prístup zamestnancov k internetových stránkam a aplikáciám, ktoré primárne nepotrebujú na výkon svojej práce.[177] Potreba kontroly výkonu práce zamestnanca zo strany zamestnávateľa je o to viac príznačná pri výkone domáckej práce a telepráce. Aplikačným problémom pri domáckej práci a telepráci je však to, akým spôsobom správne nastaviť obmedzenie prehliadania určitých internetových stránok a aplikácií, aby toto obmedzenie neprimeraným spôsobom nezasahovalo alebo

[175] BARANCOVÁ, H.: Práva zamestnancov v Európskej únie. 1.vyd. Praha: Leges, 2016, 140 s.,ISBN: 978-80-7502-117-5.
[176] MORÁVEK, J.: Ochrana osobních údaju v pracovněprávních vztazích. 1. Vyd. Praha: WoltersKluwer ČR, 2013., 436 s., ISBN: 978-80-7478-139-1.
[177] KRIŽAN, V.: Ochrana súkromia zamestnanca v ére internetu. In: BARANCOVÁ, H., OLŠOVSKÁ, A. (eds.): Súčasný stav a nové úlohy pracovného práva. Zborník vedeckých príspevokov z medzinárodnej konferencii Trnavské právnické dni. Trnava. 2016, Praha: Leges, 2016, 260 s. a nasl., ISBN: 978-80-7502-176-2.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

neobmedzovalo práva zamestnanca. Na tento aplikačný problém možno nazerať v dvoch rovinách. Prvú rovinu predstavuje situácia, kedy zamestnávateľ informoval zamestnanca o obmedzeniach používania technického a programového vybavenia. V takomto prípade akákoľvek kontrola zo strany zamestnávateľa, ktorej účelom je preverenie, ktoré internetové stránky a aplikácie zamestnanec navštívil, bude predstavovať neprimeraný zásah do súkromia zamestnanca. Druhú rovinu celej problematiky tvoria situácie, kedy zamestnávateľ informoval zamestnanca v súlade s § 52 ods. 2 pís. c) Zákonníka práce o obmedzeniach používania technického a programového vybavenia, ako aj o prípadných sankciách. V prípade, ak zamestnanec pri telepráci využíva technické vybavenie zamestnávateľa, s prípadným obmedzením používania technického vybavenia a následnou kontrolou technického vybavenia zo strany zamestnávateľa za účelom jeho správneho využívania v súlade s podmienkami dohodnutými v pracovnej zmluve nebude problém. Problém s obmedzením využitia technického vybavenia, ako aj s následnou kontrolou zameranou zo strany zamestnávateľa na dodržiavania zmluvne dohodnutých obmedzení môže nastať vtedy, ak zamestnávateľ udelil súhlas zamestnancovi na využívanie jeho technického vybavenia pri telepráci. V takomto prípade prichádza do úvahy len dohoda medzi zmluvnými stranami pracovnej zmluvy týkajúca sa vymedzenia časového úseku, v rámci ktorého zamestnanec nebude navštevovať internetové stránky a využívať aplikácie, ktoré priamo nesúvisia s výkonom jeho práce. Vymedzenie časového úseku, v rámci ktorého nebude zamestnanec navštevovať internetové stránky a využívať aplikácie, ktoré priamo nesúvisia s výkonom jeho práce, sa nám javí viac ako problematické a to z toho dôvodu, že zamestnanec vykonávajúci domácku prácu alebo teleprácu si rozvrhuje svoj pracovný čas sám. Samotný výkon kontroly takýchto obmedzení zo strany zamestnávateľa je rovnako tak otázky, pretože zamestnávateľ nemá vlastnícke právo ani užívacie právo k technickému vybaveniu, na ktorom zamestnanec vykonáva svoju prácu. Zákonník práce nám nedáva odpoveď na to, aké prípadné sankcie si môže zamestnávateľ so zamestnancom dohodnúť za to, že zamestnanec pri výkone telepráce nerešpektuje obmedzenia používania technického a programového vybavenia. Ako už bolo nami naznačené, zamestnávateľ si nemôže zo zamestnancom dohodnúť zmluvnú pokutu vzhľadom na zásadu *numerus clausus*. Je však potrebné zdôrazniť, že akákoľvek zmluvne legitímne dohodnutá sankcia nemôže byť dohodnutá len vo vzťahu k jednému konkrétnemu

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zamestnancovi, ale vo vzťahu k všetkým zamestnancom vykonávajúcim teleprácu, ako aj vo vzťahu k zamestnancom, ktorí pracujú u zamestnávateľa na pracovisku. V opačnom prípade by pracovné podmienky znevýhodňovali zamestnancov vykonávajúcich teleprácu od zamestnancov, ktorí pracujú u zamestnávateľa na jeho pracovisku.

5.7.3 Monitorovanie zamestnancov GPS systémom

S rozvojom technických prostriedkov, ktoré umožňujú zamestnávateľovi kontrolu pohybu zamestnancov patrí určite aj GPS systém. Pri využití GPS systému zo strany zamestnávateľa opäť platí, že ak GPS systém zasahuje neoprávnene do súkromnej sféry zamestnanca, porušuje tým dôstojnosť zamestnanca a to najmä v takých prípadoch, ak je zamestnanec vykonávajúci domácku prácu oprávnený podľa pracovnej zmluvy využívať svoj osobný automobil, avšak pohyb zamestnanca GPS systém monitoruje neustále, pričom takýto zamestnanec nemá v čase použitia osobného automobilu na súkromné účely možnosť deaktivovať GPS systém.[178]

5.7.3.1 Charakteristika GPS systému

Monitorovanie zamestnancov v cestnej doprave prostredníctvom GPS systému (*z angl.: „Global Positing System“*) v súčasnej dobe patrí medzi najrozšírenejšie formy monitorovania zamestnancov v cestnej doprave. Tento spôsob monitorovania zamestnancov sa stal u väčšiny verejných dopravných prostriedkov ich pravidelnou súčasťou. Podstatou GPS systému je, že umožňuje zamestnávateľovi sledovať a vyhodnocovať pomocou príslušného počítačového programu rýchlosť motorového vozidla, lokalizovať aktuálnu polohu motorového vozidla, pracovný čas a dobu odpočinku vodiča motorového vozidla a s tým súvisiace údaje. Pokým z technického hľadiska pri inštalácii a používaní GPS systému sa v aplikačnej praxi zo strany zamestnávateľov nevyskytujú výraznejšie problémy, tak z pohľadu ústavného práva a pracovného práva v kontexte ochrany súkromia zamestnanca predstavuje monitorovanie zamestnancov prostredníctvom GPS systému aplikačný problém.

5.7.3.2 Podmienky monitorovania zamestnancov

[178] BARANCOVÁ, H. a kol.: Ochrana zamestnanca, súčasnosť a budúcnosť pracovného práva. 1. vyd., Bratislava: Sprint dva, 2012, 54 s., ISBN: 978-80-89393-66-4.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Hmotnoprávne podmienky na monitorovanie zamestnancov GPS systémom vo všeobecnosti upravuje ustanovenie § 13 ods. 4 Zákonníka práce. Pokiaľ sa zamestnávateľ rozhoduje zaviesť do služobného motorového vozidla GPS systém, v prvom rade si musí odpovedať na otázku, či existujú na jeho strane vážne dôvody spočívajúce v osobitnej povahe jeho činnosti. Vážne dôvody spočívajúce v osobitnej povahe činnosti zamestnávateľa predstavujú tzv. *condicio sine qua non* na to, aby mohol zamestnávateľ monitorovať svojich zamestnancov.

Najčastejšie sa inštalácia GPS systému do motorových vozidiel odôvodňuje ekonomickými dôvodmi na strane zamestnávateľa v kontexte optimalizácie daňových výdavkov alebo ochranou majetku zamestnávateľa pred odcudzením alebo poškodením zo strany tretích osôb. Ďalším legitímnym dôvodom inštalácie GPS systému do motorových vozidiel je zvýšenie bezpečnosti a ochrany zdravia pri práci zamestnancov v cestnej doprave a eliminácia dopravných nehôd v kontexte vzniku pracovných úrazov samotných zamestnancov pracujúcich u zamestnávateľa.[179]

Vážne dôvody na strane zamestnávateľa by mali byť naplnené v prípadoch, keď zamestnávatelia poskytujú svoje služby v rámci sektora verejnej dopravy alebo ktorí využívajú pri poskytovaní svojich tovarov a služieb osobnú alebo nákladnú cestnú dopravu. Osobitnú povahu činnosti je potrebné vykladať vzhľadom ku konkrétnej pracovnej činnosti zamestnanca a nie k predmetu činnosti zamestnávateľa, ktorý je uvedený vo verejne prístupnom registri, poprípade v inom zakladajúcom dokumente zamestnávateľa ako právnickej osoby.[180]

5.7.3.3 Pracovisko zamestnanca

V druhom rade je potrebné zodpovedať otázku, či narušenie súkromia zamestnanca prostredníctvom GPS systému sa uskutočňuje na pracovisku zamestnávateľa alebo v spoločných priestoroch zamestnávateľa. Zákonník práce pojem *„pracovisko“* nevymedzuje. Za pracovisko treba podľa odbornej literatúry považovať určitý priestor, v ktorom má zamestnanec vykonávať svoju prácu. Môže ním byť napríklad príslušná kancelária, dielňa,

[179] SISKOVIČOVÁ, K.: Ochrana súkromia a osobných údajov zamestnanca, 1. vyd., Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, 149 s., ISBN: 978-80-8082-932-2.
[180] MORÁVEK, J.: Možnosti monitorování zaměstnanců na pracovišti v právním řádu České republiky. In: BARANCOVÁ, H. a kol. Monitorovanie zamestnancov a právo na súkromný život, Bratislava: Sprint dva, 2010, str. 36 a nasl., ISBN: ISBN 978-80-89393-43-5.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

stavenisko.[181] V aplikačnej praxi veľmi často dochádza k zámene pojmov *„pracovisko“* zamestnanca a *„miesto výkonu práce zamestnanca“*. V tejto súvislosti poukazujeme na rozhodnutie Najvyššieho súdu Českej republiky, ktorý zdôraznil rozdiel medzi týmito dvomi pojmami pracovného práva. Za *„miesto výkonu práce“* možno rozumieť obec, vyšší územný celok, územie Slovenskej republiky, organizačnú jednotku alebo miesto, v ktorom sa zamestnanec v pracovnej zmluve zaviazal k výkonu dohodnutého druhu práce pre zamestnávateľa. Za *„pracovisko zamestnanca“* možno považovať miesto, kde zamestnanec v súlade s pracovnou zmluvou podľa pokynov zamestnávateľa plní svoje pracovné úlohy.[182] Podľa § 8 ods. 4 písm. d) zákona o organizácii pracovného času v doprave sa pracoviskom mobilného zamestnanca v doprave rozumie aj dopravný prostriedok, ktorý mobilný zamestnanec využíva na vykonávanie dopravných činností. Podľa predmetného ustanovenia je definícia pracoviska naviazaná na definíciu mobilného zamestnanca v cestnej doprave.

5.7.4 Mobilný zamestnanec v cestnej doprave

Podľa § 7 ods. 1 zákona o organizácii pracovného času v doprave sa za *„mobilného zamestnanca v cestnej doprave“* považujú vodiči a ďalší členovia cestujúceho personálu, ktorí vykonávajú dopravné činnosti v cestnej doprave pre zamestnávateľa v pracovnom pomere. Zo samotnej definície *„mobilného zamestnanca v cestnej doprave“* je možné vyvodiť, že právne normy uvedené v zákone o organizácii pracovného času v doprave sa budú vzťahovať len na tých zamestnancov, ktorí vykonávajú závislú vo vzťahu k zamestnávateľovi v pracovnom pomere. Pracovný pomer sa zakladá výlučne písomnou pracovnou zmluvou. Pracovný pomer nemožno založiť na základe jednej z dohôd o vykonaní práce mimo pracovný pomer v zmysle § 223 a nasl. Zákonníka práce.[183] Právnym následkom konštrukcie právnej normy, ktorá spája status *„mobilného zamestnanca v cestnej doprave“* výlučne s pracovným pomerom je vznik aplikačného problému, ktorý súvisí s výkonom závislej práce zamestnancov na základe jednej z dohôd o vykonaní prác mimo pracovného pomeru. Pri analýze ustanovenia § 7 ods. 1 zákona

[181] BARANCOVÁ, H., SCHRONK, R.: Pracovné právo. Druhé prepracované a doplnené vydanie. Bratislava: Sprint 2, 2013, str. 259, ISBN: 978-80-89393-97-8.
[182] Rozhodnutie NS ČR, sp.zn.: 21 Cdo 4596/2014 zo dňa 26.11.2015.
[183] TOMAN, J: Individuálne pracovné právo. Všeobecné ustanovenia a pracovná zmluva. Bratislava: Friedrich Ebert Stifung, 2014, str. 155, ISBN: 978-80-89149-42-4.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

o organizácii pracovného času v doprave prichádzajú do úvahy dva právne výklady. Obsahom prvého právneho výkladu je teória, ktorá pracovný pomer ako podmienku statusu *„mobilného zamestnanca v cestnej doprave“* vzťahuje na ďalších členov cestujúceho personálu a na základe zlučovacej spojky *„a“* aj na vodičov cestných dopravných prostriedkov. Právnym následkom aplikácie gramatického výkladu je, že za mobilných zamestnancov v cestnej doprave sa nebudú považovať zamestnanci, ktorí vykonávajú závislú prácu na základe jednej z dohôd o vykonaní prác mimo pracovný pomer. Obsahom druhého výkladu predmetného ustanovenia je právny názor, ktorý podmienku pracovného pomeru vzťahuje len na ďalších členov cestujúceho personálu a na vodičov nie, pretože zákon o organizácii pracovného času v doprave umožňuje výkon činnosti profesionálneho vodiča aj v rámci statusu osoby samostatne zárobkovo činnej podľa § 10 zákona o organizácii pracovného času v doprave. Sme toho názoru, že takýto výklad predmetného ustanovenia je neprípustný, pretože v zmysle § 10 ods. 1 zákona o organizácii pracovného času v doprave, ktorý ustanovuje, že: *„ak ďalej nie je ustanovené inak, ustanovenia o mobilných zamestnancoch v cestnej doprave sa vzťahujú aj na samostatne zárobkovo činných vodičov.“*, nie je možné analogicky vyvodiť právny záver, že samostatne zárobkovo činní vodiči sa budú automaticky považovať za mobilných zamestnancov v cestnej doprave. Súčasne samostatne zárobkovo činní vodiči nevykonávajú prácu pre zamestnávateľa v pracovnoprávnom vzťahu, ale na základe obchodnoprávneho vzťahu. Súčasne je potrebné zdôrazniť, že zamestnávateľ by mal uzatvárať dohody o vykonaní práce mimo pracovného pomeru so zamestnancami len výnimočne. Zákonník práce však nedáva jednoznačnú odpoveď na otázku, či slovné spojenie *„výnimočne“* sa vzťahuje na časový rozmer uzatvárania dohôd alebo na charakter prác, ktoré nie sú klasickým predmetom činnosti zamestnávateľa.[184]

Uvedený legislatívny problém by mohol byť vyriešený pomocou *analógie legis*, avšak aplikácia *analógie legis* v prospech vymedzenia pracoviska sa komplikuje v prípadoch, ak sa napríklad jedná o zamestnanca, ktorý má v pracovnej zmluve dohodnutý ako druh práce *„vodič – operátor“* alebo sa jedná o *„vodiča referenta“*, ktorý nemá v pracovnej zmluve dohodnutý

[184] ŠVEC, M. a kol.: Kultúra sveta práce. Závislá práca a dohody o prácach vykonávaných mimo pracovného pomeru. Bratislava: Fridrich Ebert Stiftung, 2012, str. 22, ISBN: 978-80-89149-23-0.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

výkon práce *„vedenie motorového vozidla“* a ktorý vedie motorové vozidlo len v rámci pracovnej cesty.

5.7.4.1 Informačná povinnosť zamestnávateľa a súhlas zamestnanca

Pokiaľ zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia ako aj dobe jej trvania. Z uvedeného vyplýva, že zamestnávateľ je povinný pred monitorovaním zamestnancov prerokovať monitorovanie u zástupcov zamestnancov. Pokiaľ u zamestnávateľa nepôsobia zástupcovia zamestnancov, zamestnávateľ môže konať samostatne. Súčasne je ale povinný splniť si informačnú povinnosť voči zamestnancom. Zákonník práce vo všeobecnosti neurčuje formu prerokovania konkrétnej problematiky so zástupcami zamestnancom. Z uvedeného dôvodu k prerokovaniu problematiky monitorovania zamestnancov môže dôjsť aj neformálnym spôsobom ústne. Je však vhodné, aby zamestnávateľ a zástupcovia zamestnancov o prerokovaní spísali zápisnicu. Súčasne informačná povinnosť zamestnávateľa voči zamestnancov sa môže uskutočniť ústnou formou, čo možno považovať za negatívum právnej úpravy.

Na monitorovanie zamestnanca sa v zmysle § 13 ods. 4 Zákonníka práce súhlas nevyžaduje. Táto skutočnosť však nevylučuje, že zamestnávateľ v aplikačnej praxi nebude potrebovať súhlas od zamestnanca. Pokiaľ zamestnávateľ udelí v pracovnej zmluve súhlas na používanie súkromného motorového vozidla zamestnanca na pracovnoprávne účely a súčasne má záujem o inštaláciu GPS systému do vozidla zamestnanca, mal by si od zamestnanca vyžiadať súhlas s inštaláciou GPS systému do jeho vozidla. Ak zamestnanec takýto súhlas zamestnávateľovi udelí, nie je podľa nášho názoru automaticky možné takýto prejav vôle zamestnanca považovať za súhlas s monitorovaním zamestnanca počas pracovného času a ani za súhlas s monitorovaním fyzickej osoby mimo rámca pracovného času v zmysle § 11 Občianskeho zákonníka. V tomto prípade bude dôležitá formulácia prejavu vôle zamestnanca v pracovnej zmluve alebo v inej dohode v rámci občianskoprávneho vzťahu. Obdobná situácia môže nastať vtedy, ak zamestnávateľ udelí zamestnancovi súhlas s používaním súkromného motorového vozidla na pracovné účely, avšak uvedené vozidlo nie je vo vlastníctve zamestnanca.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Pokiaľ zamestnanec udelí zamestnávateľovi súhlas s inštaláciou GPS systému do svojho súkromného motorového vozidla alebo sa jedná o vozidlo vo vlastníctve zamestnávateľa, realizáciu monitorovania aktuálnej polohy vozidla so zamestnancom by mal zamestnávateľ realizovať výlučne v pracovnej zmene zamestnanca. Pokiaľ zamestnávateľ udelil súhlas zamestnancovi s využitím jeho motorového vozidla mimo pracovnú zmenu, môže zamestnanec za účelom ochrany súkromia deaktivovať GPS systém do režimu *„súkromná jazda“*, ak zamestnanec aktuálne využíva motorové vozidlo po skončení jeho pracovnej zmeny na súkromné účely. Toto právo zamestnancovi patrí aj keby používal svoje súkromné motorového vozidlo. Ak by sa zamestnanec v pracovnej zmluve zaviazal, že GPS systému mimo pracovnej zmeny neprepne do režimu *„súkromná jazda“*, takáto dohoda by bola absolútne neplatná pre rozpor s dobrými mravmi, pričom by bola hodnotená ako vzdanie sa práva zamestnanca na súkromný život.

Z ustanovenia § 13 ods. 4 Zákonníka práce priamo nevyplýva, kedy môže zamestnávateľ monitorovať zamestnancov a preto je potrebné odpovedať na otázku, či môže zamestnávateľ monitorovať zamestnancov počas celej pracovnej zmeny alebo len počas pracovného času, prípadne doby odpočinku. Význam hľadania odpovede na túto otázku vidíme v situácii, ak zamestnanec vedie služobné motorové vozidlo na pracovnej ceste, ktorá sa podľa Zákonníka práce nepovažuje za pracovný čas, aj keby sa podľa Smernice 2003/88/ES za pracovný čas zamestnanca považovať mala.[185]

Pri skúmaní tohto aplikačného problému je potrebné každý jeden prípad skúmať samostatne. Pokiaľ sa zamestnávateľ rozhodne monitorovať zamestnanca GPS systémom počas trávenia doby odpočinku, musí mať na to vážny prevádzkový dôvod spočívajúci v osobitnej povahe činnosti zamestnávateľa, ktorý môže spočívať napríklad v prevencii pred neoprávneným odcudzením dopravného prostriedku alebo dodržiavaním bezpečnosti a ochrany zdravia pri práci zamestnanca. Pri takomto spôsobe zásahu do súkromia zamestnanca by zamestnávateľ nemohol použiť ekonomický dôvod odôvodňujúci takýto zásah. Z uvedeného dôvodu je

[185] KRIŽAN, V.: Pracovná cesta vs. pracovný čas vyslaného zamestnanca, str. 91. In: VOJTKO, J.: Ochrana zamestnancov pri ich vyslaní do krajín Európskeho hospodárskeho priestoru. Zborník príspevkov z on-line konferencie. Trnava: Trnavská univerzita v Trnave, Právnická fakulta, 2015, 109 s., ISBN: 978-80-8082-936-0.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

dôležité, aby zamestnávatelia kládli dôraz na vymedzenie dôvodov, pre ktoré sa rozhodnú monitorovať zamestnancov.

Ďalší aplikačný problém súvisí s pracoviskom zamestnanca v cestnej doprave v kontexte možnosti monitorovať zamestnanca aj počas doby odpočinku. Je potrebné si položiť otázku, ktorá časť dopravného prostriedku (*napríklad kamiónu*) tvorí pracovisko zamestnanca. Je celkom bežné, že kabína kamióna sa skladá z dvoch častí, pričom zadná časť kamióna je prispôsobená pre vodiča na trávenie dennej alebo týždennej doby odpočinku. Sme toho názoru, že pokiaľ je kabína kamiónu vybavená kamerovým systémom, ktorého súčasťou môže byť aj GPS systému, kamerový systém by rozhodne nemal mať možnosť zaznamenávať priestor zadnej kabíny kamióna, kde vodiči trávia doby odpočinku.

S kabínou vodiča ako pracoviskom zamestnanca je spojený aplikačný problém, ktorý súvisí so zodpovedaním otázky, či môže dôjsť k narušeniu súkromia zamestnanca aj vtedy, ak by zamestnávateľ monitoroval priestor kabíny bez prítomnosti zamestnanca počas trávenia doby odpočinku. Z hľadiska právneho skúmania celej problematiky je podstatné, či môže za istých okolností tvoriť kabína vodiča ako pracovisko zamestnanca súkromie zamestnanca bez jeho osobnej prítomnosti. Pokiaľ by súčasťou kabíny vodiča kamiónu boli veci, ktoré by umožnili zamestnávateľovi zistiť napríklad jeho náboženské vyznanie alebo sexuálnu orientáciu, tak priestor kabíny dopravného prostriedku môže za takýchto okolností byť súčasťou súkromia zamestnanca.

5.7.5 Právo zamestnanca odpojiť sa

Na zamestnanca vykonávajúceho teleprácu sa podľa § 52 ods. 1 Zákonníka práce nevzťahujú ustanovenia o rozvrhnutí týždenného pracovného času, nepretržitom dennom odpočinku, nepretržitom odpočinku v týždni a o prestojoch, ale vzťahujú sa na zamestnanca ustanovenia o maximálnom týždennom pracovnom čase zamestnanca podľa § 85 Zákonníka práce. Zamestnanec si síce rozvrhuje pracovný čas sám, avšak jeho pracovný čas nie je neobmedzený. V pracovnej zmluve sa môže zamestnávateľ so zamestnancom dohodnúť, kedy musí byť zamestnanec prítomný pri komunikačných prostriedkoch doma, aby bol zastihnuteľný a bol k dispozícii pre zamestnávateľa. V aplikačnej praxi sa však stáva, že takíto zamestnanci sú

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

nútení vybavovať rôzne záležitosti súvisiace s ich výkonom práce aj v neskorých večerných hodinách alebo počas víkendov a štátnych sviatkov. S týmto aplikačným problémom súvisí tzv. právo zamestnanca odpojiť sa (*right to disconnect*). Súčasťou reformy pracovného zákonodarstva vo Francúzsku je zavedenie práva byť *offline* pre zamestnancov, ktorí počas vopred stanoveného časového úseku nebudú musieť z domova odpovedať na e-maily, sms správy alebo dvíhať mobilné telefóny. Uvedené právo nemajú všetci zamestnanci, ale len zamestnanci, korí pracujú u zamestnávateľa, ktorý zamestnáva viac ako 50 zamestnancov.[186] Toto právo na jednej strane ochraňuje zamestnancov, avšak na druhej strane môže u nich vyvolať pocit zahltenosti a obavu z toho, že po uvedenom časovom úseku budú zahltení sms správami alebo e-mailami, ktoré budú musieť vybaviť. S postupnou liberalizáciou pracovnoprávnych vzťahov by bolo vhodné, aby právna úprava výkonu domáckej práce a telepráce zakotvila pre zamestnancov právo *right to disconnect*. Za zmienku však stojí myšlienka, či by sa takéto právo nemalo vzťahovať na všetkých zamestnancov *en bloc*. Je síce pravdou, že v súčasnej dobe podľa Zákonníka práce zamestnanci nemusia vybavovať e-maily ani sms správy po pracovnej dobe, avšak v mnohých prípadoch sú zo strany zamestnávateľov zamestnanci nútení, aby aj po pracovnej dobe odpovedali na e-maily alebo sms správy.

5.8 KONTROLA VECÍ

Pracovné právo upravuje vzťahy, v rámci ktorých môže dochádzať k značným stratám na životoch, zdraví, majetku, prírode i životnom prostrední. Kladie dôraz na to, aby sa pracovný proces nestal zdrojom ohrozenia alebo porušenia právom chránených záujmov. Pre naplnenie tejto idey vytvára samostatný prevenčný systém, ktorý vychádza z klasickej zásady nikomu neškodiť (*neminem laedere*).

Prevenciou rozumieme súhrn činností, práv a povinností vopred zameraných na zabránenie vzniku škody. Na rozdiel od Občianskeho zákonníka č. 40/1964 Zb., ktorý túto otázku upravuje iba rámcovo, je celý systém v pracovnoprávnych predpisoch rozpracovaný pomerne dôsledne.

[186] Bližšie pozri: https://www.theguardian.com/money/2016/dec/31/french-workers-win-legal-right-to-avoid-checking-work-email-out-of-hours (prezerané dňa 08.02.2017, 17:42 hod.)

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Pravidlá sú formulované od všeobecných právnych predpisov tak, aby pokryli čo najväčší okruh pracovných vzťahov - situácií, až po ostatné predpisy, v ktorých je povinnosť detailne konkretizovaná, podľa ustanovenia § 39 Zákonníka práce č. 311/2001 Z.z. (ZP).

Prevencia sa rozdeľuje podľa účelu, ktorý sleduje, na generálnu a špeciálnu.[187]

Generálna všeobecne smeruje k odvráteniu možného ohrozenia alebo porušenia práv a povinností subjektov pracovnoprávnych vzťahov.

Špeciálna zas sleduje odstránenie príčiny hroziacej škody v konkrétnom prípade a Zákonník práce k tomu stanovuje aj určité povinnosti.

Oba druhy sa uskutočňujú celým radom rozličných právnych prostriedkov, ktoré sa prejavujú opatreniami slúžiacimi prevencii buď priamo alebo nepriamo. Prvoradým a v podstate jediným zmyslom priamych preventívnych opatrení je predchádzanie škodám, zatiaľ čo opatrenia nepriamej prevencie upravujú správanie subjektov všeobecne tak, aby sa zabránilo ohrozeniu alebo poškodzovaniu práv a povinností, ktoré tvoria obsah pracovnoprávnych vzťahov, ale ich hlavným cieľom je úprava iného inštitútu.

Prevencii je v pracovnom práve priznaná taká dôležitosť, že popri kontrole prostredníctvom zástupcov zamestnancov existuje aj vonkajšia kontrola vykonávaná príslušnými štátnymi orgánmi odborného dozoru ako prejav verejného záujmu.

Účelom prevenčného opatrenia vyjadreného v § 177 ods. 2 ZP je ochrana majetku zamestnávateľa pri výkone práce: „Na ochranu svojho majetku je zamestnávateľ oprávnený vykonávať v nevyhnutnom rozsahu kontrolu vecí, ktoré zamestnanci vnášajú na pracovisko alebo odnášajú z pracoviska. Podrobnejšie podmienky určí zamestnávateľ v pracovnom poriadku. Pri kontrole sa musia dodržať predpisy o ochrane osobnej slobody a nesmie byť ponižovaná ľudská dôstojnosť.“

Kontrola môže pozostávať nielen zo zisťovania obsahu tašiek, ale jej súčasťou môže byť aj osobná prehliadka zamestnanca, vrátane previerky detektorom kovov. Jej realizácia musí zodpovedať nevyhnutnému rozsahu v odôvodnených prípadoch akými sú podozrenia z

[187] Viac GALVAS, M. in GALVAS, M. a kol.: *Pracovní právo.* Vyd. 1. Brno : Masarykova univerzita, 2012, s. 601.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

krádeže majetku zamestnávateľa alebo vnášanie nebezpečných predmetov na pracovisko, ktoré môžu ohroziť nielen životy a zdravie osôb, ale aj majetok zamestnávateľa.

Realizovať sa môže nielen priamo na pracovisku, ale podľa konkrétnych podmienok aj v iných priestoroch ako napr. miesto vstupu do objektu zamestnávateľa. V tejto spojitosti prof. Olšovská zdôrazňuje, že kontrola vecí a prehliadky sa môžu uskutočňovať len v pracovnom čase. Ak by sa konali vo voľnom čase zamestnanca, zamestnávateľ by konal v rozpore s účelom uvedeného ustanovenia.[188]

Nedostatkom je textácia ustanovenia, keď sa obmedzuje iba na ochranu majetku zamestnávateľa (*„Na ochranu svojho majetku je zamestnávateľ oprávnený...*“). V praxi môžu nastať rôzne situácie pri ochrane majetku iného, kedy nebude jednoducho možné ho aplikovať. Napr. ak zamestnávateľ nadobudne podozrenie, že jeho zamestnanec-čašník okradol zákazníka v reštaurácií. Namiesto širšej interpretácie, že § 177 ods. 2 ZP pokrýva aj nepriamu ochranu majetku zamestnávateľa (napr. krádežou veci hosťovi personálom môže vzniknúť škoda v majetkovej sfére zamestnávateľa, ak si hosť uplatní právo na náhradu škody), by bolo vhodnejšie legislatívne vypustiť privlastňovacie zámeno 'svojho' a nechať formuláciu vo všeobecnej rovine.[189]

Ustanovenie explicitne zakotvuje, že musia byť dodržiavané predpisy o ochrane osobnej slobody a nesmie byť ponižovaná ľudská dôstojnosť. Pod osobnou slobodou, ktorú zaručuje Čl. 17 Ústavy Slovenskej republiky, sa rozumie voľný, ničím neobmedzený pohyb jednotlivca, ktorý sa môže podľa vlastného rozhodnutia zdržiavať na určitom mieste alebo slobodne z tohto miesta odísť.

Protektívnej funkcie pracovného práva sa týka aj nezasahovanie do ľudskej dôstojnosti zamestnanca ako najvyššej ochranyhodnej hodnoty. Právo kontroly musí byť v súlade s dobrými mravmi, nesmie byť vykonávaný šikanóznym spôsobom a na ujmu zamestnanca. S tým súvisí aj to, že osobnú prehliadku môže vykonať iba fyzická osoba rovnakého pohlavia, aj

[188] OLŠOVSKÁ, A. in BARANCOVÁ, H. a kol.: *Pracovný pomer a poistný systém*. Bratislava : Typi Universitatis Tyrnaviensis, vydavateľstvo Trnavskej univerzity, Veda - Vydavateľstvo Slovenskej akadémie vied, 2008, s. 413.
[189] Rovnako MORÁVEK, J.: O vhodnosti a o nevhodnosti novelizace Zákoníku práce. In GREGOROVÁ, Z. (ed.): Pracovní právo 2016 : Zákoník práce v novelizaci, důchodová reforma v akci Brno : Masarykova univerzita, 2017, s. 50.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

keď v praxi sa to niektorým autorom javí ako komplikované riešenie, keďže zamestnávateľ zamestnávajúci mužov aj ženy musí zabezpečiť, aby kontrola bola vykonávaná aspoň jedným zástupcom mužského a jedným zo ženského pohlavia.[190]

Rešpektované musí byť právo zamestnanca na ochranu jeho osobnosti v rozsahu ustanovenia § 11 Občianskeho zákonníka. V prípade porušenia osobnostných práv by sa zamestnanec mohol domáhať postupom podľa § 13 Občianskeho zákonníka predovšetkým, aby sa upustilo od neoprávnených zásahov do práva na ochranu jeho osobnosti, aby sa odstránili následky týchto zásahov a aby mu bolo dané primerané zadosťučinenie. Pokiaľ by sa nezdalo postačujúce uvedené zadosťučinenie a najmä preto, že bola v značnej miere znížená jeho dôstojnosť alebo vážnosť v spoločnosti, má tiež právo na náhradu nemajetkovej ujmy v peniazoch. Výšku náhrady by určil súd s prihliadnutím na závažnosť vzniknutej ujmy a na okolnosti, za ktorých k porušeniu práva došlo.

Zamestnávateľ môže svoje právo uskutočňovať sám, ale aj za pomoci iných subjektov, napr. strážnych služieb alebo bezpečnostných agentúr, ktoré vykonávajú kontrolu na základe zmluvného vzťahu a splnomocnenia udeleného zamestnávateľom.[191] Za prípadne konanie v rozpore s analyzovaním ustanovením bude stále zodpovedať zamestnávateľ.

Na predchádzanie nejasnostiam pracovnoprávny kódex zakotvuje, že podmienky pri kontrole vecí zamestnávateľ určí podrobnejšie v pracovnom poriadku. Napriek výslovnej zmienke nejde o určenie povinnosti upraviť tieto záležitosti v internom normatívnom akte. Ide len o odporúčanie, ktorého formulácia v texte zákona je nadbytočná, pretože právo prijať vnútorný predpis je prejavom zamestnávateľovej organizačnej právomoci. Dôležité je tiež zdôrazniť, že v prípade sporu nebude pracovný poriadok právne významný a pôjde iba o skutkovú okolnosť, ktorá môže spolu s ďalšími skutočnosťami prispieť k obsahu súdneho rozhodnutiu.

5.9 OSOBNÝ SPIS

[190] SISKOVIČOVÁ, K.: *Ochrana súkromia a osobných údajov zamestnanca*. Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, s. 78.
[191] VYSOKAJOVÁ, M. – KAHLE, B. – DOLEŽÍLEK, J.: *Zákoník práce s komentářem*. Praha: ASPI, a. s. 2007, s. 317.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Zamestnávateľ nie je povinný viesť osobný spis, avšak je ťažké si predstaviť, že by sa zaobišiel bez aspoň základnej evidencie údajov.

Napriek významu je v Zákonníku práce č. 311/2001 Z.z. (ZP) zmienený iba v štvrtej vete § 75 ods. 1: *„Zamestnanec má právo nahliadnuť do osobného spisu a robiť si z neho výpisy, odpisy a fotokópie.“*

To je zrejme aj dôvod prečo tejto problematike nie je venovaná príliš veľká pozornosť na úrovni základnej výkladovej literatúry. Napr. v najnovšom komentári nie je k osobnému spisu ani slovo.[192] V inom je úsporná informácia, ktorá nereflektuje všetky situácie, ktoré môžu nastať: *„Zamestnávateľ má strpieť, aby zamestnanec mohol nahliadnuť do svojho osobného spisu a robiť si z neho odpisy, výpisy a fotokópie. Podľa existujúceho právneho stavu má zamestnanec právo získať potrebné informácie zo svojho osobného spisu a zamestnávateľ je povinný mu to umožniť. Namiesto aktívneho správania má zamestnávateľ podľa súčasného právneho stavu umožniť výkon práva zamestnanca. Bolo by vhodné, aby uvedené oprávnenie zamestnanca bolo konkretizované v pracovnom poriadku. Najmä u zamestnávateľov s vysokým počtom zamestnancov* by *realizácia uvedeného oprávnenia zamestnanca mohla spôsobiť problémy. Výkon práva zamestnanca robiť si odpisy, výpisy a fotokópie z osobného spisu neznamená, že zamestnávateľ je povinný robiť zamestnancovi fotokópie z osobného spisu. Dikcia ustanovenia „robiť si z neho odpisy, výpisy a fotokópie“ predpokladá, že ich bude robiť sám zamestnanec, a nie zamestnávateľ.“*[193]

Naopak, v Českej republike je prístup iný. Najmä Morávek podáva rozšírený rozbor[194], čo zaiste súvisí s precíznejším právnym rámcom.[195]

---

[192] ŠVEC, M. - TOMAN, J. a kol.: Zákonník práce. Zákon o kolektívnom vyjednávaní ; komentár zväzok 1 čl. 1 až § 176 Zákonníka práce. Bratislava: Wolters Kluwer, 2019. 1479 s.

[193] RYBÁROVÁ, M. in BARANCOVÁ, H. a kol.: Zákonník práce : komentár. 2. vyd. Bratislava : C.H. Beck, 2019, s. 748.

[194] MORÁVEK, J. in PICHRT, J. a kol.: Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář. Praha: Wolters Kluwer, 2017.

[195] § 312 Zákoník práce č. 262/2006 Sb.:
„(1) Zaměstnavatel je oprávněn vést osobní spis zaměstnance. Osobní spis smí obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu uvedeném v § 3.
(2) Do osobního spisu mohou nahlížet vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni. Právo nahlížet do osobního spisu má orgán inspekce práce, Úřad práce České republiky, Úřad pro ochranu osobních údajů, soud, státní zástupce, policejní orgán, Národní bezpečnostní úřad a zpravodajské služby. Za nahlížení do osobního

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

5.9.1 Forma a obsah osobného spisu

Vzhľadom na to, že zákon neurčuje formu, môže byť spis vedený v materializovanej, digitalizovanej alebo kombinovanej verzii. Často sa možno stretnúť s jeho uložením na externý server (úložiská), ktorý nepatrí zamestnávateľovi.[196]

Právna úprava ani nevymedzuje konkrétne údaje, ktoré môžu byť vkladané do osobného spisu. Čo je obsahom *„diktuje samotná prax a jej zaužívané postupy, z čoho je zrejmé, že (...) nebude u jednotlivých* zamestnancov *totožný“*[197]. Zásadným limitom je Článok 11 Základných zásad ZP, podľa ktorého *„[z]amestnávateľ môže o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával“*.

O rozsahu a druhu rozhoduje zamestnávateľ podľa vlastného uváženia pri zohľadnení svojich zákonných povinností a oprávnených záujmov a potrieb a to všetko pri minimalizovaní zásahov do súkromia zamestnanca v intenciách čl. 19 ods. 2 a 3 a 22 ods. 2 Ústavy Slovenskej republiky, ako i čl. 8 Dohovoru o ochrane ľudských práv a základných slobôd a čl. 7 a čl. 8 Charty základných práv Európskej únie.

Pôjde najmä o personálnu a mzdovú agendu, pri ktorej zamestnávateľ dodržiava povinnosti uložené rôznymi právnymi predpismi. Hlavným prameňom údajov je nielen ZP a súvisiace pracovnoprávne predpisy, ale aj predpisy z oblastí daní či sociálneho zabezpečenia.

---

spisu se nepovažuje předložení jednotlivé písemnosti zaměstnavatelem z tohoto spisu vnějšímu kontrolnímu orgánu, který provádí kontrolu u zaměstnavatele a který si tuto písemnost vyžádal v souvislosti s předmětem kontroly prováděné u zaměstnavatele.
(3) Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele.“

[196] Pozri viac VARGA, V.: Náhrada škody a nemajetkovej ujmy dotknutej osoby pri úniku jej (nielen) zdravotných údajov z cloudu. In: Starostlivosť o zdravie zamestnancov. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2018, s. 346: *„[P]okiaľ zamestnávateľ vedie osobný spis zamestnanca v cloude, má zamestnávateľ postavenie prevádzkovateľa 6 v zmysle ZOOÚ (GDPR), externá spoločnosť zabezpečujúca personalistiku zasa postavenie sprostredkovateľa; to všetko s náležiacimi právami a povinnosťami. Pokiaľ osobný spis zamestnanca vedie sprostredkovať a využíva pri tom cloudové služby, poskytovateľ cloudových služieb má postavenie ďalšieho sprostredkovateľa (subdodávateľa).“*

[197] BARINKOVÁ, M. - ŽUĽOVÁ, J: Elektronizácia pracoviska s akcentom na ochranu práva zamestnanca a zamestnávateľa. In: Právo, obchod, ekonomika VI. : zborník príspevkov z vedeckej konferencie. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2016, s. 42.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

V zložke budú bežné informácie, ktoré sa nevyhnutne vzťahujú na osobou zamestnanca, najmä meno a priezvisko, trvalý alebo prechodný pobyt, adresa na doručovanie, názov zdravotnej poisťovne, bankové spojenie a ich zmeny, ako i o listiny nevyhnutné pre výkon práce ako žiadosť o zamestnanie, životopis, osobný dotazník, doklady o dosiahnutom vzdelaní, kvalifikácií, praxi, a ostatných oprávneniach alebo schopnostiach (napr. vodičské oprávnenie alebo zbrojný preukaz), pracovná zmluva, pracovný posudok a potvrdenie o zamestnaní z predchádzajúcich zamestnaní, súhlas s výkonom inej zárobkovej činnosti, výzvy na odstránenie nedostatkov, upozornenia na možnosť výpovede, dohoda o zvýšení kvalifikácie, dohoda o hmotnej zodpovednosti, potvrdenie o zverení predmetov, dohoda o zrážkach zo mzdy, evidencia dochádzky a iné.

Do spisu sa zakladajú buď rovnopisy alebo fotokópie s poznámkou, že boli porovnané s originálom. Nie je potrebné uchovávať v spise všetky doklady preukazujúce relevantné informácie, keďže je zamestnanec kedykoľvek povinný preukázať správnosť tvrdených skutočností potrebných pre plnenie zákonných povinností zamestnávateľa. Podľa povahy informácie k tomu môže často stačiť, aby v osobnom spise bolo uvedené kto a na základe akých dokumentov údaje overil. V tejto spojitosti zamestnávateľ musí brať aj ohľad na osobné údaje tretích osôb, ktoré sa môžu nachádzať na listinách predkladaných zamestnancom. Takéto údaje nemôže zamestnávateľ zakladať do spisu, a to ani keby s tým zamestnanec súhlasil.[198]

Obsahom spisu nemôžu byť ani rôzne podania a sťažnosti iných osôb, ktoré sa netýkajú pracovného vzťahu zamestnávateľa a zamestnanca. Súčasťou spisu by v zásade nemali byť ani lekárske záznamy vzťahujúce sa na fyzické alebo psychické zdravie, ani informácie, ktoré nie sú potrebné na plnenie povinností zamestnávateľa; pôjde predovšetkým o tie, ktoré zamestnávateľ nesmie vyžadovať od fyzickej osoby v rámci predzmluvných vzťahov v zmysle § 41 ods. 6 ZP, t.j. o tehotenstve, o rodinných pomeroch, o bezúhonnosti (s výnimkou, ak ide o prácu, pri ktorej sa podľa osobitného predpisu vyžaduje bezúhonnosť, alebo ak požiadavku

[198] Viac pozri MATES, P. – JANEČKOVÁ, E. – BARTÍK, V.: Ochrana osobních údajů. Praha : Leges, 2012, s. 82.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

bezúhonnosti vyžaduje povaha práce, ktorú má fyzická osoba vykonávať), o politickej príslušnosti, odborovej príslušnosti, náboženskej príslušnosti.[199]

Je nesporné, že zamestnávateľ môže a musí pri plnení svojich povinností získavať aj citlivé informácie o zamestnancovi, ako napr. lekárske potvrdenie o tehotenstve, či lekársky posudok o dlhodobej strate spôsobilosti naďalej vykonávať doterajšiu prácu. V takýchto prípadoch bude dôvod získania údajov legitímny, ale po oboznámení sa s nimi, musí ich zaradenie a uchovávanie v osobnom spise zodpovedať rozsahu nevyhnutnému na dosiahnutie účelu ich spracovania, t.j. pre potreby výkonu závislej práce. Aj za týchto okolností platí zásada rovnakého zaobchádzania, a teda zamestnanec nesmie byť na základe získaných informácií žiadnym spôsobom diskriminovaný.

5.9.2 Právo zamestnanca na prístup k údajom, ktoré sa ho týkajú

Kontrola zo strany zamestnanca o údajoch, ktoré o ňom zamestnávateľ vedie, stojí na dvoch pilieroch. Prvý vychádza zo štvrtej vety § 75 ods. 1 ZP. Pracovnoprávna úprava vychádza z ústavného práva na informačné sebaurčenie. Jej účelom je transparentná kontrola zo strany zamestnanca, aké záznamy o ňom vedie zamestnávateľ.

Druhým je nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (GDPR), a to najmä Článok 15:

„1. Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a tieto informácie:

a) účely spracúvania;

b) kategórie dotknutých osobných údajov;

[199] Uvedené ustanovenie je ďalej rozšírené aj o ďalšie informácie v zmysle § 62 ods. 3 zákona č. 5/2004 Z. z. o službách zamestnanosti.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

c) príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie;

d) ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;

e) existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu;

f) právo podať sťažnosť dozornému orgánu;

g) ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj;

h) existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

2. Ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa článku 46 týkajúcich sa prenosu.

3. Prevádzkovateľ poskytne kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

4. Právo získať kópiu uvedenú v odseku 3 nesmie mať nepriaznivé dôsledky na práva a slobody iných.“

5.9.3 Právo nahliadnuť do osobného spisu podľa ZP

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Pracovnoprávna regulácia je previazaná s osobným spisom, ktorý spravidla vedie každý zamestnávateľ, aj keď mu zákon takúto povinnosť priamo neukladá. Ide o jednu alebo viac zložiek o zamestnancovi a nie je podstatné, či ich zamestnávateľ označuje ako osobný spis. Osobitné alebo pridružené súbory, bez ohľadu na to, kde sa uchovávajú, sú tiež jeho súčasťou. *„Ak má zamestnávateľ väčší počet zamestnancov, niektoré dokumenty, ktoré sa týkajú konkrétneho* zamestnanca*, nemusia byť súčasťou jedného osobného spisu, ale môže ich viesť hromadne pre viacerých zamestnancov podľa predmetu spracúvania ich osobných údajov (napr. dokumenty, týkajúce sa bezpečnosti a ochrany zdravia pri práci).“*[200]

V zložke budú bežné informácie, ktoré nevyhnutne súvisia s osobou zamestnanca, najmä meno a priezvisko, trvalý alebo prechodný pobyt, adresa na doručovanie, názov zdravotnej poisťovne, bankové spojenie a ich zmeny, ako i listiny nevyhnutné pre výkon práce ako žiadosť o zamestnanie, životopis, osobný dotazník, doklady o dosiahnutom vzdelaní, kvalifikácií, praxi, a ostatných oprávneniach alebo schopnostiach (napr. vodičské oprávnenie alebo zbrojný preukaz), pracovná zmluva, pracovný posudok a potvrdenie o zamestnaní z predchádzajúcich zamestnaní, súhlas s výkonom inej zárobkovej činnosti, výzvy na odstránenie nedostatkov, upozornenia na možnosť výpovede, dohoda o zvýšení kvalifikácie, dohoda o hmotnej zodpovednosti, potvrdenie o zverení predmetov, dohoda o zrážkach zo mzdy, evidencia dochádzky a iné.[201]

So zreteľom na to, že realizácia analyzovaného práva nie je bližšie upravená, je vhodné konkretizovať ju v pracovnom poriadku[202] pri zohľadnení osobitných podmienok zamestnávateľa. Zamestnávateľ je povinný strpieť výkon zamestnancovho práva, ktorý musí byť v súlade s dobrými mravmi. Pri šikanóznom konaní môže zamestnávateľ s odkazom na §

[200] SISKOVIČOVÁ, K.: Ochrana súkromia a osobných údajov zamestnanca. Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, s. 122-123.
[201] Pozri tiež BARINKOVÁ, M. - ŽUĽOVÁ, J: Elektronizácia pracoviska s akcentom na ochranu práva zamestnanca a zamestnávateľa. In: Právo, obchod, ekonomika VI. : zborník príspevkov z vedeckej konferencie. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2016, s. 43.
[202] RYBÁROVÁ, M. in BARANCOVÁ, H. a kol.: Zákonník práce : komentár. 2. vyd. Bratislava : C.H. Beck, 2019, s. 748.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

13 ods. 3 ZP[203] výkon práva nahliadnuť do osobného spisu obmedziť alebo zamestnancovi nevyhovieť v celom rozsahu.

Momentom vytvorenia osobného spisu je zvyčajne založenie pracovného pomeru. Nemožno vylúčiť ani skorší okamih už počas výberu zamestnancov. V takomto prípade je však otázne, či uchádzačovi o zamestnanie patrí právo podľa § 75 ZP. Skôr sa prikláňam k tomu, že nie každý dokument obsahujúci údaje o dotknutej osobe (napr. žiadosť o zamestnanie, životopis) ihneď spadá pod pojem osobný spis v zmysle ZP.

Nazerať do osobného spisu a robiť z neho výpisy, odpisy a fotokópie smie len zamestnanec v pracovnom pomere. Primárne sa to týka aktuálnych, ale v primeranej miere sa to vzťahuje aj na bývalých zamestnancov, najmä na tých krátko po skončení pracovného pomeru.[204]

Stretnúť sa možno s názorom, že do osobného spisu môže nahliadať vedúci zamestnanec, alebo dokonca osoba príslušná na zúčtovanie mzdy ako napr. účtovníčka, mzdová personalistka. Autor síce priznáva, že takéto oprávnenie explicitne nevyplýva zo znenia zákona, ale je možné ho vyvodiť z postavenia vedúceho zamestnanca (§ 9 ods. 3 ZP) či z jeho povinností (§ 239 písm. b/ ZP).[205] Takéto široké ponímanie ide proti celkovému cieľu analyzovaného ustanovenia, ktoré je potrebné vykladať reštriktívne. Bez výslovného vyjadrenia v ZP[206] nie je možné rozširovať právo nazerať do osobného spisu na iné osoby vrátane zástupcov zamestnancov (11a ods. 1 ZP).

Prístup tretích osôb do osobného spisu zamestnanca nie je úplne vylúčený, ale získavanie údajov (a teda aj nahliadanie) musí byť umožnené osobitným právnym predpisom (napr. ZoOÚ) alebo striktne viazané na oprávnený dôvod (napr. príslušné orgány policajného zboru).

---

[203] § 13 ods. 3 ZP: *„Výkon práv a povinností vyplývajúcich z pracovnoprávnych vzťahov musí byť v súlade s dobrými mravmi. Nikto nesmie tieto práva a povinnosti zneužívať na škodu druhého účastníka pracovnoprávneho vzťahu alebo spoluzamestnancov. Nikto nesmie byť na pracovisku v súvislosti s výkonom pracovnoprávnych vzťahov prenasledovaný ani inak postihovaný za to, že podá na iného zamestnanca alebo zamestnávateľa sťažnosť, žalobu, návrh na začatie trestného stíhania alebo iné oznámenie o kriminalite alebo inej protispoločenskej činnosti.“*

[204] Bližšie k úprave osobného spisu pozri PORUBAN, A.: Pracovný posudok, potvrdenie o zamestnaní a osobný spis zamestnanca. In Súkromné právo, 2/2018, s. 74-80.

[205] VARGA, V.: Mzda ako osobný údaj. In: Právne nástroje odmeňovania v 21. storočí. Bratislava : Friedrich Ebert Stiftung, 2017. s. 70.

[206] Porovnaj s § 312 ods. 2 českého Zákoníku práce.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Domnievam sa, že zamestnanec ani nemôže na nahliadnutie udeliť plnomocenstvo splnomocnencovi, a to ani advokátovi, pretože ide o osobné právo úzko späté s jeho súkromím.

Realizácia nahliadania nie je bližšie normatívne upravená. Možno ju však konkretizovať v pracovnom poriadku pri zohľadnení osobitných podmienok každého zamestnávateľa zvlášť. Zamestnávateľ je povinný strpieť výkon zamestnancovho práva, ktorý musí byť v súlade s dobrými mravmi. Pri šikanóznom konaní môže zamestnávateľ s odkazom na § 13 ods. 3 ZP výkon práva nahliadnuť do osobného spisu obmedziť alebo zamestnancovi nevyhovieť v celom rozsahu.

Zamestnávateľ poskytuje súčinnosť a sprístupňuje spis alebo jeho časti na vyžiadanie zamestnanca. Dáva mu pri tom k dispozícii dostatočný časový priestor adekvátny objemu požadovaných dát v mieste, kde sa osobný spis obvykle uchováva.

V zásade platí, že diať by sa tak malo v priebehu pracovného času zamestnanca. Ak to však prevádzkové dôvody zamestnávateľa alebo povaha práce zamestnanca neumožňujú, tak aj počas doby odpočinku. Kontrola údajov sa môže uskutočniť za prítomnosti zamestnávateľa alebo ním poverenej osoby z dôvodu povinnosti zamestnávateľa chrániť dáta pred stratou, poškodením alebo ich zmenou.

Zamestnávateľ nie je povinný vyhotovovať kópie záznamov nachádzajúcich sa v spise. Zamestnanec si ich môže robiť sám, a to na vlastné náklady; údaje nesmie odstraňovať, meniť ani inak znehodnocovať. V tejto súvislosti bude pre zamestnanca lepšie využiť právo na kópie údajov podľa Článku 15 ods. 3 GDPR, ktoré je nezávislé od práva na prístup k informáciám podľa ods. 1.[207]

V prípade zistenia porušenia práv môže využiť nástroje, ktoré mu patria podľa GDPR resp. ZoOÚ, akými sú právo na opravu, výmaz alebo obmedzenie nesprávnych, neúplných či neaktuálnych osobných údajov, ktoré sú predmetom spracúvania, alebo v zmysle ochrany osobnostných práv podľa § 13 Občianskeho zákonníka, a to najmä upustenie od

[207] Pozri poznámku pod čiarou č. 11.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

neoprávnených zásahov, odstránenie následkov, poskytnutie primeraného zadosťučinenia, náhrada nemajetkovej ujmy.

Trvanie vedenia závisí od druhu jednotlivých údajov v ňom obsiahnutých. Doba uchovávania je stanovená buď osobitnými právnymi predpismi, prípadne zamestnávateľ spis vedie do uplynutia všetkých do úvahy pripadajúcich prekluzívnych a objektívnych premlčacích lehôt. *„Osobný spis zamestnanca, vedený zamestnávateľom, môže mať podľa zákona č. 395/2002 Z. z. archívnu hodnotu a po jeho odovzdaní (v súlade so schváleným registratúrnym plánom) do príslušného archívu je k osobným údajom, v ňom obsiahnutým, obmedzený prístup po dobu 90 rokov od vzniku záznamu. Osobný spis zamestnanca je vhodné uchovávať minimálne po dobu, ako sú uchovávané ročné mzdové listy, t. j. 50 rokov.“*[208]

5.9.4 Právo na prístup k údajom podľa GDPR

Zamestnanec sa môže dožadovať informácií o údajoch spracovávaných zamestnávateľom aj podľa GDPR. Článok 15 ods. 1 výslovne uvádza, že má právo získať od zamestnávateľa potvrdenie, či osobné údaje, ktoré sa ho týkajú sú alebo nie sú spracúvané, a pokiaľ tomu tak je, má právo získať prístup k ním.

Týka sa to osobných údajov v zmysle Článku 4 bod 1 GDPR: „Na účely tohto nariadenia 'osobné údaje' sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len 'dotknutá osoba'); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.“ Môže ísť o údaje, ktoré uložené v osobnom spise, ale aj o iné, ako napr. záznamy z firemnej kroniky alebo fotografie z teambuildingu.[209]

Vzhľadom na to, že v pracovnoprávnych vzťahoch sa osobné údaje generujú vo veľkom rozsahu a po dlhú dobu, zamestnanec musí vysvetliť, ktorých informácií alebo

[208] ŽUĽOVÁ, J. – ŠVEC, M.: GDPR a ochrana záujmov zamestnanca. Bratislava : Friedrich Ebert Stiftung, 2018, s. 96.
[209] ŽUĽOVÁ, J. – ŠVEC, M.: GDPR a ochrana záujmov zamestnanca. Bratislava : Friedrich Ebert Stiftung, 2018, s. 56.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

spracovateľských činností sa jeho žiadosť týka v zmysle odôvodnenia č. 63 veta 7 GDPR: „*Ak prevádzkovateľ spracúva v súvislosti s dotknutou osobou veľké množstvo informácií, mal by môcť požadovať, aby pred doručením informácií dotknutá osoba spresnila, ktorých informácií alebo spracovateľských činností sa žiadosť týka*.“ Aj žiadosť ohľadom 'výkonnosti', 'plnenia pracovných úloh', či 'správania' bude dostatočne konkrétna, pretože zamestnanec nie je spravidla schopný vopred bližšie špecifikovať informácie, ktoré o ňom zamestnávateľ spracúva.[210]

Zamestnanec nemá právo na prístup k informáciám iba ak sa týkajú legitímnych záujmov ostatných zamestnancov alebo tretích osôb v zmysle Článku 23 ods. 1 písm. i) GDPR: „*V práve Únie alebo práve členského štátu, ktorému prevádzkovateľ alebo sprostredkovateľ podliehajú, sa prostredníctvom legislatívneho opatrenia môže obmedziť rozsah povinností a práv ustanovených v článkoch 12 až 22 a v článku 34, ako aj v článku 5, pokiaľ jeho ustanovenia zodpovedajú právam a povinnostiam ustanoveným v článkoch 12 až 22, ak takéto obmedzenie rešpektuje podstatu základných práv a slobôd a je nevyhnutným a primeraným opatrením v demokratickej spoločnosti s cieľom zaistiť ochranu dotknutej osoby alebo práv a slobôd iných.*“ Je na zamestnávateľovi, aby zvážil proporcionalitu medzi konkrétnym záujmom na poskytnutí informácie na jednej strane a záujmom o jej utajenie na strane druhej. Pri odmietnutí práva na informácie však musí predložiť relevantné skutočnosti.

V intenciách Článku 15 ods. 3 GDPR má zamestnanec tiež právo na kópie údajov. Použitý pojem 'kópia' evokuje, že by malo ísť o exemplár získaný prepísaním alebo rozmnožovacou technikou, duplikát či napodobeninu. V súlade s účelom GDPR je potrebné tento termín vnímať ako zmysluplné štruktúrované zhrnutie rozpoznateľných osobných údajov, ktoré spracováva zamestnávateľ.

Ani pri práve podľa ods. 3 nesmú byť nepriaznivo dotknuté práva a slobody iných osôb. A keďže nejde o oddelené právo od ods. 1, obmedzenie podľa Článku 15 ods. 4 GDPR sa za

[210] Pozri rozhodnutie Landesarbeitsgericht Baden-Württemberg z 20.12.2018. sp. zn. 17 Sa 11/18.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

použitia argumentu *a minori ad maius* vzťahuje nielen na právo na kópiu, ale aj na právo na prístup k údajom podľa ods. 1.[211]

Práva zamestnanca podľa ods. 1 aj 3 musia tiež zodpovedať požiadavke stručnosti, transparentnosti, zrozumiteľnosti, dostupnosti, jasnosti a jednoduchosti v zmysle Článku 12 GDPR.

Článok 15 GDPR môže byť východiskom aj pre ďalšie práva, ako napr. na opravu (Článok 16 GDPR), na vymazanie (Článok 17 GDPR) alebo na obmedzenie spracúvania (Článok 18 GDPR).

Právny rámec prístupu k údajom podľa ZP nie je ideálny. Okrem toho, že úprava vedenia osobného spisu je veľmi stručná, hlavným nedostatkom je fakt, že nahliadať nemôžu zamestnanci v pracovnoprávnych vzťahoch založených niektorou z dohôd o prácach vykonávaných mimo pracovného pomeru podľa § 223 ZP[212]. Toto by dalo vyriešiť jednoduchým legislatívno-technickým opatrením - vyňatím štvrtej vety z § 75 ods. 1 ZP, ktorá sa vzťahuje iba na zamestnancov v pracovnom pomere, a jej presunutím medzi všeobecné ustanovenia ZP.

Na druhej strane zamestnanci nielen v pracovnom pomere, 'dohodári', bývalí zamestnanci, uchádzači o zamestnanie, ale aj rodinní príslušníci a blízke osoby zamestnanca, či akékoľvek ďalšie osoby, majú k dispozícii alternatívu – GDPR, ktorá poskytuje vhodné nástroje ako efektívne realizovať výkon práva na informačné sebaurčenie.

Navyše, vecná pôsobnosť GDPR je širšia a pokrýva aj informácie o výkonnosti, plnení pracovných úloh či správaní zamestnanca, a to aj napriek tomu, že tieto pojmy nie sú priamo definované v Článku 4 bod 1 GDPR ako osobný údaj. Spadať však budú pod Článok 15 ods. 1 písm. b) GDPR, t.j. 'kategórie dotknutých osobných údajov'.

---

[211] Porovnaj s PAAL, P. - PAULY, D.A.: Datenschutz-Grundverordnung Bundesdatenschutzgesetz. 2. Auflage. München : C.H.BECK, 2018.

[212] § 223 ZP ods. 1: „Zamestnávateľ môže na plnenie svojich úloh alebo na zabezpečenie svojich potrieb výnimočne uzatvárať s fyzickými osobami dohody o prácach vykonávaných mimo pracovného pomeru (dohodu o vykonaní práce, dohodu o pracovnej činnosti a dohodu o brigádnickej práci študentov), ak ide o prácu, ktorá je vymedzená výsledkom (dohoda o vykonaní práce) alebo ak ide o príležitostnú činnosť vymedzenú druhom práce (dohoda o pracovnej činnosti, dohoda o brigádnickej práci študentov). Podmienka výnimočnosti podľa prvej vety sa nevzťahuje na dohodu o pracovnej činnosti na výkon sezónnej práce podľa § 228a ods. 1 písm. b).“

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

V neposlednom rade výhodou GDPR, aj keď ide len o náhodný vedľajší účinok, je aj to, že získané informácie môžu slúžiť ako podklady na uplatňovanie nárokov na náhradu škody alebo nemajetkovej ujmy podľa iných predpisov.

5.10 PREDKLADANIE SPRÁV O DOHODNUTÝCH NOVÝCH PRACOVNÝCH POMEROCH

Podľa § 47 ods. 4 ZP je zamestnávateľ povinný predkladať zástupcom zamestnancov správy o dohodnutých nových pracovných pomeroch v lehotách, ktoré s ním dohodol. Ide o rozšírenie práva zástupcov zamestnancov na informácie v zmysle § 238 ZP.[213]

Zamestnávateľ plní svoju povinnosť buď k odborovej organizácii, zamestnaneckej rade alebo zamestnaneckému dôverníkovi; povinnosť nemá vo vzťahu k zástupcovi zamestnancov pre bezpečnosť a ochranu zdravia pri práci. Ak u zamestnávateľa nepôsobia zástupcovia zamestnancov, povinnosť predkladať správy o dohodnutých nových pracovných pomeroch odpadá.

V prípade, že nie sú dohodnuté žiadne lehoty, musí zamestnávateľ plniť svoju povinnosť bez zbytočného odkladu po vzniku pracovného pomeru. To znamená, že nie odo dňa založenia pracovného pomeru (= uzavretie pracovnej zmluvy), ale odo dňa, ktorý bol dohodnutý ako deň nástupu do práce.

Povinnosť sa vzťahuje nielen na pracovné pomery na neurčitý čas, ale aj na určitú dobu i kratší pracovný čas.

Vzhľadom na to, že ide o lehotu a nie dobu (v zmysle § 37 ZP), lehota určená podľa dní začína sa dňom, ktorý nasleduje po udalosti, ktorá je rozhodujúca pre jej začiatok. Koniec lehoty určenej podľa týždňov, mesiacov alebo rokov pripadá na deň, ktorý sa pomenovaním alebo číslom zhoduje s dňom, na ktorý pripadá udalosť, od ktorej sa lehota začína. Ak nie je takýto deň v poslednom mesiaci, pripadne koniec lehoty na jeho posledný deň. Ak posledný deň

[213] § 238 ZP:
„(1) Informovanie je poskytnutie údajov zamestnávateľom zástupcom zamestnancov s cieľom oboznámenia sa s obsahom informácie.
(2) Zamestnávateľ informuje zrozumiteľným spôsobom a vo vhodnom čase zástupcov zamestnancov o svojej hospodárskej a finančnej situácii a o predpokladanom vývoji jeho činnosti.
(3) Zamestnávateľ môže odmietnuť poskytnúť informácie, ktoré by mohli poškodiť zamestnávateľa, alebo môže vyžadovať, aby sa tieto informácie považovali za dôverné.“

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

lehoty pripadne na sobotu, nedeľu alebo sviatok, je posledným dňom lehoty najbližší nasledujúci pracovný deň (§ 122 Občianskeho zákonníka č. č. 40/1964 Zb.).

Zamestnávateľ sa nemôže zbaviť tejto povinnosti s odkazom na ochranu osobných údajov, pretože spracúvanie je nevyhnutné na splnenie právnej povinnosti prevádzkovateľa v súlade s Článkom 6 ods. 1 písm. c) všeobecného nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane údajov (GDPR).

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

6 VÝNIMKY ZO ZÁSAHOV DO OCHRANY SÚKROMIA ZAMESTNANCOV

Právnym základom pre obmedzenie práva na súkromie, zakotvuje čl. 8 ods. 2 Európskeho Dohovoru, pričom uvedené ustanovenie predstavuje ***tzv. limitačnú klauzulu***. Podľa predmetného ustanovenia Európskeho dohovoru platí, že zásah či obmedzenie do práva na ochranu súkromia je možné len v prípade, ak je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinom, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných. Jedná sa o štandardnú limitačnú klauzulu.[214]

Charta upravuje možnosť obmedzenia ňou zaručených práv v článku 52. Podľa tohto článku Charta pripúšťa obmedzenie základných práv a slobôd nej upravených a to na základe Charty samotnej, ďalej na základe medzinárodných zmlúv týkajúcich sa organizácie EÚ a súčasne na základe princípov vyjadrených v Európskom dohovore. Podľa článku 52 ods. 1 Charty platí, že: *„akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných.“* Súčasne podľa článku 52 ods. 2 Charty platí, že: *„práva uznané v tejto charte, ktoré sú predmetom ustanovení zmlúv, sa vykonávajú za podmienok a v medziach vymedzených týmito zmluvami.“* Uvedené ustanovenie predstavuje možnosť obmedzenia základných práv a slobôd na základe medzinárodných zmlúv týkajúcich sa organizácie EÚ. Na záver je potrebné uviesť, že podľa článku 52 ods. 3 Charty platí, že: *„v rozsahu, v akom táto charta obsahuje práva, ktoré zodpovedajú právam zaručeným v Európskom dohovore o ochrane ľudských práv a základných slobôd, zmysel a rozsah týchto práv je rovnaký ako zmysel a rozsah práv ustanovených v uvedenom dohovore. Toto ustanovenie nebráni tomu, aby právo Únie priznávalo širší rozsah ochrany týchto práv.“* Uvedený článok Charty predstavuje limitáciu a obmedzenie základných práv a slobôd

[214] KMEC, J., KOSAŘ, D., KRATOCHVÍL, J., BOBEK, M.: Evropská úmluva o lidských právech. Komentář. Praha: C .H. Beck, 2012, str. 99.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

uvedených v Charte na základe vyššie spomenutých princípov zakotvených v Európskom dohovore.

Možnosť obmedzenia ochrany súkromia zamestnancov možno nájsť v Ústave SR ako aj v Listine základných práv a slobôd. Generálna klauzula obmedzení základných práv a slobôd vyjadrených v Ústave SR je zakotvená v článku 13 Ústavy SR. Podľa článku 13 ods. 1 Ústavy SR platí, že: *„povinnosti možno ukladať a) zákonom alebo na základe zákona, v jeho medziach a pri zachovaní základných práv a slobôd; b) medzinárodnou zmluvou podľa čl. 7 ods. 4, ktorá priamo zakladá práva a* povinnosti *fyzických osôb alebo právnických osôb; alebo c) nariadením vlády podľa čl. 120 ods. 2.“* V zmysle článku 13 ods. 2,3 a 4 Ústavy SR platí, že: *„medze základných práv a slobôd možno upraviť za podmienok ustanovených touto ústavou len zákonom. Zákonné obmedzenia základných práv a slobôd musia platiť rovnako pre všetky prípady, ktoré spĺňajú ustanovené podmienky. Pri obmedzovaní základných práv a slobôd sa musí dbať na ich podstatu a zmysel. Takéto obmedzenia sa môžu použiť len na ustanovený cieľ.“*

Listina upravuje generálnu klauzulu limitácie a obmedzenia základných práv a slobôd vo svojom článku 4. Možnosť zásahu do základných ľudských práv a slobôd na základe článku 4 Listiny je možný len na základe zákona a zákonné obmedzenia základných práv a slobôd musia platiť pre všetky prípady, ktoré spĺňajú ustanovené podmienky. Pri používaní ustanovení o medziach základných práv a slobôd sa musí dbať o ich podstatu a zmysel. Takéto obmedzenia základných práv a slobôd sa nesmú zneužívať na iné účely, než na ktoré boli ustanovené.

Na základe vyššie uvedeného právneho základu obmedzení a limitácie základných ľudských práv a slobôd môžeme vyvodiť právny záver, že právo na ochranu súkromia zamestnanca ako základné ľudské právo možno obmedziť zásahom do tohto práva len po splnení troch kritérií, ktorými sú kritérium ***legality, legitimity a proporcionality.***

Podľa aktuálnej rozhodovacej činnosti Ústavného súdu SR k problematike testu legality, legitimity a proporcionality uviedol, že: *„zásahy do právna na súkromie sa v zmysle judikatúry vykladajú v určitej logickej nadväznosti a postupnosti. Je potrebné predovšetkým skúmať, či*

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

daný skutkový stav možno považovať za súčasť práva na súkromie. Po kladnej odpovedi na túto otázku treba skúmať*, či bol legálny. V ďalšom kroku je potrebné skúmať, či bol zásah do práva na súkromie legitímny a napokon, či bol aj proporcionálny. Ak sa následne dospeje k negatívnej odpovedi pri niektorej z týchto otázok, ďalej sa už v skúmanej problematike nepokračuje."*[215]

6.1 KRITÉRIUM LEGALITY

Zásah do práva na súkromný život zamestnanca je možný uskutočniť výlučne len na zákonnom základe. Zákonný právny základ zásahu do práva na súkromný život zamestnanca môže mať podobu písaného alebo nepísaného práva. Uvedené platí aj podľa Európskeho dohovoru. Zákonný podklad na zásah do práva na ochrany súkromia zamestnanca musí byť dostatočne jasný a určitý. Ide o právne vyjadrenie zásady legality, bez splnenia ktorej bude akýkoľvek zásah do práva na ochranu súkromia vyhodnotený ako nezákonný, ktorý nemá oporu v platnej legislatíve. Podľa rozhodovacej činnosti Ústavného súdu SR plne súladnej s aktuálnou judikatúrou ESĽP kritérium legality znamená, že štát môže zasiahnuť do práva na ochranu súkromia len vtedy, ak takýto zásah zákon pripúšťa a právna norma ho upravuje dostatočne jasne a určito na to, aby bol za ustanovených podmienok predvídateľný.[216] Oprávnený zásah do práva na súkromný život zamestnanca na základe kritéria legality je rovnako tak vyjadrený v Európskom dohovore ako aj v Charte, pričom uvedené kritérium je rovnako tak v slovenskej legislatíve upravené v Ústave SR ako aj v Listine.[217] Nesmie ísť o akýkoľvek zákon, ale uvedený zákon musí spĺňať materiálne náležitosti, ktoré vo svojej podstate predstavujú spravodlivý zákon, resp. spravodlivé a racionálne právo.

Pri zisťovaní naplnenia pojmu legalita je potrebné skúmať aj to: „či k zásahu do práva na ochranu súkromia došlo v súlade s príslušnými právnymi predpismi, pričom je potrebné prihliadnuť na to, či bol právny predpis verejne publikovaný a dostupný, a či jeho právne

---

215 Rozhodnutie Ústavného súdu SR, sp. zn.: I. ÚS 274/05

216 Uznesenie Ústavného súdu SR sp. zn.: II 280/09-16 zo dňa 10.09.2009.

217 BARANCOVÁ, H.: Práva zamestnancov Európskej únie. Praha: Leges, 2016, str. 142, ISBN: 978-80-7502-117-5.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

následky boli predvídateľné. V konkrétnom prípade je potrebné skúmať aj kvalitu zákonnej úpravy, ktorá je základom do práva na súkromie.“ 218

6.2 KRITÉRIUM LEGITIMITY

Kritérium legitimity v podstate vyjadruje, že sa musí jednať o legitímny cieľ zásadu do súkromného života zamestnanca. Legitímnosť zásahu do práva na súkromie je spojená s jeho účelom, ktorý je bližšie definovaný v článku 8 ods. 2 Európskeho dohovoru, teda zásah do práva na ochranu súkromia je prípustný vtedy, ak:

a) je to v záujme štátu z dôvodu ochrany národnej bezpečnosti, verejnej bezpečnosti, predchádzania nepokojom a zločinom;

b) je to v záujme spoločnosti z dôvodu zabezpečenia hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinom, ochrany zdravia alebo morálky;

c) je to v záujme jednotlivcov z dôvodu ochrany práv a slobôd iných.[219]

Z vyššie uvedeného teda vyplýva, že kritérium legitimity je spojené s potrebou chrániť aj iné základné práva fyzických a právnických osôb alebo verejný záujem alebo štátny záujem štátu. Podľa Ústavného súdu SR: *„legitímnosť zásahu do práva na súkromie je spojená s jeho účelom, ktorý je definovaný v článku 8 ods. 2 Európskeho dohovoru, teda zásah do práva na súkromie je prípustný len vtedy, ak je to v záujme štátu z dôvodu ochrany národnej bezpečnosti, verejnej bezpečnosti, predchádzania nepokojom a zločinnosti, v záujme spoločnosti z dôvodu zabezpečenia hospodárskeho blahobytu krajiny, ochrany zdravia alebo morálky a v záujme jednotlivcov z dôvodu ochrany práv a slobôd iných.“*[220]

Vo vyššie uvedených súvislostiach s ochranou súkromia zamestnancov je teda právnou otázkou, či majetkové záujmy zamestnávateľa možno považovať za legitímny cieľ zásahu do súkromného a rodinného života zamestnanca. Sme toho názoru, že každý jeden prípad zásahu

218 Rozhodnutie Ústavného súdu SR, sp. zn.: I. ÚS 274/05.
219 Rozsudok ESĽP v právnej veci (Klass / Nemecko) z roku 1978.
220 Rozhodnutie Ústavného súdu SR, sp. zn.: II. ÚS 280/09.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

do súkromia zamestnanca je potrebné skúmať samostatne s náležitým vyhodnotením kritéria legitimity. V niektorých prípadoch zásahov môžu byť majetkové záujmy zamestnávateľa legitímnym cieľom zásahov do práva na súkromie zamestnanca napríklad tým, že zamestnávateľ zamestnanca monitoruje. Na to, aby sa v konkrétnom prípade jednalo o oprávnený a ospravedlniteľný zásah do práva na súkromie zamestnanca, je potrebné okrem dodržania kritéria legality a legitimity skúmať aj tretie kritérium, ktorým je kritérium proporcionality.

6.3 KRITÉRIUM PROPORCIONALITY

Kritérium legitimity v sebe zahŕňa požiadavku, že štát môže zasiahnuť do práva na súkromie len v tom prípade, keď je to nevyhnutné za daných okolností, legitímny cieľ nie je možné dosiahnuť inak a pri dodržaní zásad a princípov vlastných pre svoju demokratickú spoločnosť. Kritérium proporcionality má zabezpečiť, aby zásah do práva na ochranu súkromia nebol použitý vo väčšom rozsahu, v akom bolo potrebné na dosiahnutie legitímneho cieľa.

Samotné kritérium proporcionality v sebe obsahuje viaceré prvky, a to prvok vhodnosti, potrebnosti (nutnosti) a proporcionality v užšom slova zmysle. Prvok vhodnosti je zachovaný, ak obmedzujúci prostriedok či opatrenie sú spôsobilé dosiahnuť zamýšľaný cieľ a môže teda nastať i želaný účinok. Ak zamýšľané opatrenie nie je schopné dosiahnuť želateľný účinok, prvok vhodnosti nie je daný. Prvok potrebnosti je zachovaný, ak je schopný vyvolať požadovaný následok pri čo najmenšom zásahu. Ide vlastne o dodržanie kritéria ***tzv. intervenčného minima***[221], ktoré znamená, že nemohol byť využitý iný rovnako účinný prostriedok, ktorý by zasahoval do základného práva v menšom rozsahu. Prvok proporcionality v užšom slova zmysle je zachovaný, ak je zásah do základného práva pomerný s úžitkom, ktorý bol obmedzením práva v prospech iného základného práva či verejného záujmu dosiahnutý. Záťaž je teda pomerná vo vzťahu k žiadanému a dosiahnutému výsledku.[222] Test proporcionality je z pohľadu rozhodovacej činnosti súdu založený na troch

[221] WAGNEROVÁ, E., ŠIMÍČEK, V., LANGÁŠEK, T., POSPÍŠIL, I. a kol. Listina základních práv a svobod. Komentář. Praha: Wolters Kluwer, 2012, str. 27 a nasl.

[222] PRÍBELSKÝ, P., LIŠIAK, P., ČERNÁKOVÁ, J.: Ochrana súkromia na pracovisku z pohľadu ústavného práva. Plzeň: Aleš Čeněk, 2014, str. 14, ISBN: 978-80-7380-476-3.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

krokoch. Z uvedeného dôvodu sa niekedy zvykne nazývať aj ***„tzv. trojkrokovým testom proporcionality“***. Prvým krokom je test dostatočne dôležitého cieľa, v ktorom sa skúma, či zásah smeruje k cieľu, ktorý je dostatočne dôležitým na ospravedlnenie zásahu do práva na ochranu súkromia. Druhým krokom je test nevyhnutnosti, podľa ktorého sa skúma, či v konkrétnom prípade nebolo možné využiť iný prostriedok alebo šetrnejší zásah do práva na ochranu súkromia. Tretím krokom je test proporcionality v užšom slova zmysle, v rámci ktorého sa skúmajú dve skutočnosti. Prvou skutočnosťou je, praktická koordinácia a súladnosť obidvoch kolidujúcich základných práv a druhou skutočnosťou je test ***„tzv. Alexyho vážiacej formule“***, ktorý vo svojej podstate predstavuje vážiaci vzorec. Vážiaca formula pracuje s tromi stupňami hodnôt, a to *„nízka“*, *„stredná“* a *„podstatná“*. Intenzita zásahu do práva na ochranu súkromia sa pomeruje s mierou uspokojiteľnosti druhého práva v kolízii, pričom miera uspokojenia jedného práva a intenzita zásahu do druhého práva môžu nadobudnúť jednu z vyššie uvedených troch hodnôt.223

6.4 POSÚDENIE VÝNIMKY SÚDOM

Na základe vyššie uvedených skutočností môžeme uzatvoriť, že zásahy do osobného súkromia budú v súlade s právnym poriadkom, len ak sú oprávnené. Neoprávnený zásah do práva na ochranu súkromia zamestnanca možno považovať za zásah nedovolený. Samotné kritéria nedovoleného a neoprávneného zásahu do práva na ochranu súkromia zamestnanca možno zadefinovať tak, že sa v aplikačnej praxi bude jednať o zásahy, ktoré nemajú oporu v platnej a účinnej právnej úprave, ktoré nesledujú stanovený cieľ a ktoré bolo možné za daných okolností vykonať menej invazívnym a šetrnejším spôsobom, zásahy, ktoré neboli nevyhnutné na dosiahnutie sledované cieľa a pod. Samotné posúdenie, či sa v konkrétnom prípade jedná alebo nejedná o oprávnený alebo neoprávnený zásah do ochrany súkromia zamestnanca, bude v každom jednotlivom prípade vyhodnocovať súd. Súd je jediným orgánom, ktorý na základe vyššie spomínaných kritérií a testov môže s konečnou platnosťou a záväznosťou vyhodnotiť, či zásah do súkromia zamestnanca spĺňal všetky kritériá legality, legitimity a proporcionality. Je nutné uviesť, že súd pri svojom rozhodovaní nie je viazaný internými normatívnymi právnymi aktami zamestnávateľa, ktoré rôznymi spôsobmi „tzv. legalizujú“

223 Nález Ústavného súdu SR, sp. zn.: 152/08.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

monitorovanie zamestnancov na pracoviskách zamestnávateľov. Interné normatívne právny akty zamestnávateľa častokrát formálne legalizujú monitorovanie zamestnancov zamestnávateľa na pracovisku tým, že sú v nich mnohokrát upravené podmienky monitorovania zamestnancov len formálne s rôznymi prehláseniami o splnení podmienok na monitorovanie zamestnancov. Je úlohou vnútroštátnych súdov, aby na základe vyššie uvedených kritérií všetky okolnosti prípade neoprávnených zásahov do ochrany súkromia zamestnancov zvážili a vo vzájomných súvislostiach vyhodnotili tak, či konkrétny zásah do ochrany súkromia zamestnanca bol alebo nebol oprávneným zásahom do práva na ochranu súkromia zamestnanca.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

7 ROZHODOVACIA ČINNOSŤ NAJVYŠŠÍCH SÚDNYCH AUTORÍT

Vplyv digitalizácie v pracovnom práve je možné pozorovať aj pri zavádzaní nových spôsobov monitorovania zamestnancov. Zamestnávatelia majú možnosť využívať za účelom ochrany svojho majetku čoraz modernejšie a dokonalejšie technológie. Digitalizáciou však často dochádza k neoprávneným zásahom zamestnávateľa do práva na súkromný život zamestnancov. Pretrvávajúci konflikt medzi právom na súkromie zamestnanca a ochranou majetku zamestnávateľa treba preto posudzovať aj s prihliadnutím na možnosti využívania nových moderných monitorovacích prostriedkov.[224]

Rozvoj technológií je taký rýchly, že zákony častokrát nestíhajú reflektovať na nové zmeny. Pri interpretácii jednotlivých ustanovení pomáha rozhodovacia prax súdov, ktorá vnáša do tejto oblasti aspoň nejakú mieru istoty. Vzhľadom nato, že právo na ochranu súkromia zamestnancov je garantované nielen na vnútroštátnej úrovni, ale aj na úrovni medzinárodných dohovorov, v tejto oblasti je pre nás zaujímavá aj rozhodovacia prax medzinárodných súdov.

S otázkou týkajúcou sa monitoringu sa nedávno musel vysporiadať Európsky súd pre ľudské práva, keď vo veci Antović a Mirković proti Čiernej Hore posudzoval, či zavedením monitorovacieho systému do prednáškových miestností došlo k zásahu do súkromia učiteľov na Univerzite v Čiernej Hore. Vzhľadom na aktuálnosť tejto otázky aj na slovenských univerzitách, sme sa rozhodli venovať analýze tohto rozhodnutia.

7.1 PRÁVO NA SÚKROMIE

Právo na súkromie patrí medzi základné ľudské práva garantované medzinárodnými dohovormi a Ústavou Slovenskej republiky.[225] Z medzinárodných dohovorov máme na mysli najmä Dohovor o ochrane ľudských práv a základných slobôd, ktorý vo svojom článku 8 ustanovuje: „Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie“. Na úrovni práva Európskej Únie je dôležitým prameňom práva

[224] K tomu pozri bližšie: BARANCOVÁ, H.: Nové technológie v pracovnoprávnych vzťahoch. Praha: Leges, 2017, s 11-12.
[225] zákon č. 460/1992 Zb Ústava Slovenskej republiky (ďalej len „Ústava SR“)

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

predovšetkým Charta základných práv EÚ zakotvujúca právo na súkromie vo svojom článku 7 v takmer totožnom znení.

V rámci slovenskej právnej úpravy Ústava SR v článku 16 ods. 1 zaručuje nedotknuteľnosť osoby a jej súkromia a zároveň v článku 19 ods.2 garantuje právo každého na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života. S ochranou súkromia úzko súvisí aj ochrana listové tajomstva[226], ochrana osobných údajov[227] a tiež všeobecná právna úprava ochrany súkromia ako zložky osobnostných práv, ktorá je predmetom Občianskeho zákonníka[228].

Ochrana súkromia je osobitne upravená aj priamo v Zákonníku práce[229], pričom tu sa právna úprava zameriava už konkrétne na ochranu súkromia zamestnanca v pracovnoprávnych vzťahoch. Za základný právny rámec v prípade ochrany súkromia v pracovnom práve možno považovať článok 11 Zákonníka práce týkajúci sa ochrany osobných údajov zamestnanca, v zmysle ktorého môže zamestnávateľ o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával.

Právo na súkromie zamestnanca je chránené aj v §13 ods. 4 Zákonníka práce, ktorý pojednáva o zákonných možnostiach monitorovania zamestnancov na pracovisku. Zákonník práce podmieňuje monitorovanie zamestnancov splnením určitých povinností zo strany zamestnávateľa.

Prvou takouto podmienkou je existencia vážneho dôvodu, ktorý spočíva v osobitnej povahe činností zamestnávateľa. Takéto vážne dôvody je potrebné posudzovať individuálne vzhľadom na predmet činnosti zamestnávateľa. Ako príklad možno uviesť rozdielny prístup k sledovaniu elektronickej pošty v prípade zamestnávateľa, ktorý je softvérovou spoločnosťou a vyrába antivírusové programy ako v prípade zamestnávateľa, ktorého predmetom činnosti sú

[226] čl. 22 Ústavy SR
[227] najmä zákon č. 18/2018 zákon o ochrane osobných údajov a o zmene a o doplnení niektorých predpisov
[228] § 11-16 zákona č. 40/1964 Občianskeho zákonníka
[229] zákon č. 311/2001 Z. z. Zákonník práce (ďalej len „Zákonník práce“)

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

sťahovacie služby.[230] V druhom prípade, by bola existencia vážneho dôvodu spočívajúceho v osobitnej povahe činnosti zamestnávateľa len ťažko obhájiteľná pred súdom.

Druhou podmienkou vyplývajúcou z tohto ustanovenia je splnenie oznamovacie povinnosti zamestnávateľom voči zamestnancom. Zamestnávateľ je povinný vopred informovať zamestnancov o rozsahu kontroly, o spôsobe jej vykonávania a o dobe jej trvania, v opačnom prípade by šlo o nezákonný spôsob monitorovania.

7.2 JUDIKATÚRA ESĽP SÚVISIACA S OCHRANOU OSOBNÝCH ÚDAJOV

7.2.1 Rozhodovacia činnosť ESĽP a osobné údaje

Právo na ochranu osobných údajov sa uplatňuje vždy, keď sa spracúvajú osobné údaje, je preto širšie ako právo na rešpektovanie súkromného života. Každá spracovateľská operácia osobných údajov podlieha primeranej ochrane. Ochrana údajov sa týka všetkých druhov osobných údajov a spracúvania údajov bez ohľadu na vzťah so súkromím a vplyv na súkromie. Spracúvaním osobných údajov sa môže tiež porušovať právo na súkromný život, ako sa uvádza v príkladoch uvedených ďalej. Uplatňovanie pravidiel ochrany údajov si však nevyžaduje preukázanie narušenia súkromného života. Právo na súkromie sa týka situácií, v ktorých bol ohrozený súkromný záujem alebo „súkromný život“ jednotlivca. Pojem „súkromný život“ sa v judikatúre vo všeobecnosti vykladá tak, že sa vzťahuje na intímne situácie, citlivé alebo dôverné informácie, ktoré by mohli mať vplyv na to, ako jednotlivca vníma verejnosť, a dokonca na aspekty profesionálneho života a správania na verejnosti. Posúdenie existencie alebo neexistencie zásahu do „súkromného života“ však závisí od kontextu a skutkových okolností každého prípadu. Naopak, akákoľvek operácia zahŕňajúca spracúvanie osobných údajov môže patriť do rozsahu pôsobnosti pravidiel ochrany údajov a viesť k uplatneniu práva na ochranu osobných údajov. Napríklad, ak zamestnávateľ zaznamená informácie o menách zamestnancov a odmenách, ktoré im vyplatil, samotné zaznamenanie týchto informácií nemožno považovať za zásah do súkromného života. Proti takémuto zásahu by sa však mohlo namietať, ak by napríklad zamestnávateľ preniesol osobné informácie zamestnancov tretím

[230] BARANCOVÁ, H., OLŠOVSKÁ, A (eds.): Pracovné právo v digitálnej dobe. Praha: Leges, 2017, s. 70

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

osobám. Zamestnávatelia musia v každom prípade dodržiavať pravidlá ochrany údajov, pretože zaznamenávanie údajov zamestnancov predstavuje spracúvanie údajov.[231]

Rozhodovacia činnosť Európskeho súdu pre ľudské práva (ďalej ako „ESĽP“) je preto veľmi dôležitým zdrojom poznania, ako v reálnom živote dochádza k uplatňovaniu ochrany osobných údajov a či toto uplatňovanie je alebo nie v súlade s medzinárodnými dokumentmi. V rozhodovacej praxi ESĽP pritom možno badať široký posun v ochrane tohto práva, ktorý je vyvolaný novšími a sofistikovanejšími metódami, na základe ktorých možno osobné údaje získavať, spracúvať a využívať.

Technologický pokrok viedol k obrovskému skoku v sledovaní, zachytávaní komunikácie a uchovávaní údajov, čo následne viedlo k veľkým výzvam v oblasti ochrany osobných údajov. Od rozsudku vo veci *Leander proti Švédsku* z roku 1987, v ktorom ESĽP po prvýkrát analyzoval otázku uchovávania osobných údajov jednotlivca orgánom verejnej moci, zaznamenala judikatúra orgánov dohovoru v tejto oblasti významný vývoj. V priebehu ďalších rokov ESĽP preskúmal mnoho situácií, v ktorých boli otázky súvisiace s touto problematikou vznesené. Široké spektrum operácií týkajúcich sa osobných údajov, ako je zhromažďovanie, uchovávanie, používanie a šírenie takýchto údajov, je v súčasnosti pokryté judikatúrou orgánov Dohovoru.[232] Táto judikatúra sa vyvíjala v súlade s rýchlym vývojom informačných a komunikačných technológií.

Právo na ochranu osobných údajov nie je samostatným právom medzi rôznymi právami a slobodami Dohovoru. ESĽP napriek tomu uznal, že ochrana osobných údajov má zásadný význam pre užívanie práva osoby na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie, ako ho zaručuje článok 8 Dohovoru (*Satakunnan Markkinapörssi Oy a Satamedia Oy proti Fínsku* [VK[233]], 2017, § 137; *Z proti Fínsku*, 1997, § 95). Tento článok je hlavným nástrojom, prostredníctvom ktorého sú osobné údaje chránené v systéme Dohovoru,

[231] Agentúra Európskej únie pre základné práva a Rada Európy. Príručka o európskych právnych predpisoch v oblasti ochrany údajov. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021, s. 22.
[232] Dohovor o ochrane ľudských práv a základných slobôd, Oznámenie Federálneho ministerstva zahraničných vecí č. 290/1992 Zb. (ďalej len „Dohovor“).
[233] VK znamená, že ide o rozhodnutie Veľkej komory ESĽP – *pozn. autora*.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

hoci úvahy súvisiace s touto ochranou môžu prichádzať do úvahy aj podľa iných ustanovení Dohovoru a jeho protokolov.[234]

Článok 8 Dohovoru znie: Právo na rešpektovanie súkromného a rodinného života. 1. Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie. 2. Štátny orgán nemôže do výkonu tohto práva zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných

ESĽP vo svojich rozsudkoch vysvetľuje pojem „osobné údaje“ s odkazom na Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov z 28. januára 1981, ktorý nadobudol platnosť v roku 1985 a bol aktualizovaný v roku 2018[235] (ďalej len „dohovor č. 108“), ktorého cieľom je „zabezpečiť na území každej zmluvnej strany pre každého jednotlivca ... rešpektovanie jeho práv a základných slobôd, a najmä jeho práva na súkromie, pokiaľ ide o automatické spracovanie osobných údajov, ktoré sa ho týkajú“ (článok 1) (*Amann proti Švajčiarsku* [VK], 2000, § 65; *Haralambie proti Rumunsku*, 2009, § 77). ESĽP jasne uviedol, že podľa článku 2 Dohovoru 108 je pojem osobných údajov definovaný ako „akákoľvek informácia týkajúca sa identifikovanej alebo identifikovateľnej osoby“ (tamtiež).

Takéto údaje zahŕňajú nielen informácie, ktoré priamo identifikujú jednotlivca („dotknutú osobu“), ako je priezvisko a meno (*Guillot proti Francúzsku*, 1996, § 21 - 22; *Mentzen proti Lotyšsku* (odm.[236]), 2004; *Güzel Erdagöz proti Turecku*, 2008, § 43; *Hájovský proti Slovensku*, 2021, § 11-12 a 41), ale aj akýkoľvek prvok nepriamo identifikujúci osobu, ako je dynamická IP adresa (internetový protokol) (*Benedik proti Slovinsku*, 2018, § 107-108).

Osobné údaje môžu mať veľmi rôznu podobu. Judikoval to ESĽP napríklad v týchto prípadoch:

a) informácie o používateľoch internetu spojené s konkrétnymi dynamickými IP adresami pridelenými v určitom čase (*Benedik proti Slovinsku*, 2018, § 108-109),

[234] K ich úplnému zneniu pozri: https://www.echr.coe.int/documents/d/echr/convention_slk.
[235] K jeho textu pozri: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000016807c65bf.
[236] Odm. znamená, že sťažnosť bola súdom zamietnutá – *pozn. autora*.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

b) záznamy vyhotovené na použitie ako hlasové vzorky, ktoré majú trvalú povahu a podliehajú procesu analýzy priamo súvisiacej s identifikáciou osoby v kontexte iných osobných údajov (*P. G. a J. H. proti Spojenému kráľovstvu*, 2001, § 59),

c) bunkové vzorky a profily DNA (*S. a Marper proti Spojenému kráľovstvu* [VK], 2008, § 70-77) alebo odtlačky prstov (tamtiež, § 84), ktoré napriek svojej objektívnej a nevyvrátiteľnej povahe obsahovali jedinečné informácie o dotknutej osobe a umožňovali jej presnú identifikáciu za širokého spektra okolností (tamtiež, § 85),

d) informácie o danej osobe získané z bankových dokladov, či už zahŕňajú citlivé údaje alebo profesionálnu činnosť (*M. N. a ostatní proti San Marínu*, 2015, § 51 a nasl.),

e) údaje o povolaní identifikovanej alebo identifikovateľnej osoby, ktoré zhromažďuje a uchováva polícia (*Khelili proti Švajčiarsku*, 2011, § 56),

f) údaje o používaní internetu a správ (Yahoo) zamestnancom na pracovisku, získané prostredníctvom sledovania (*Bărbulescu proti Rumunsku* [VK], 2017, § 18, 74 - 81),

g) kópia elektronických údajov zaistených v advokátskej kancelárii, hoci neboli dešifrované, prepísané ani oficiálne pridelené ich vlastníkom (*Kırdök a ostatní proti Turecku,* 2019, § 36),

h) údaje zhromaždené v rámci neutajeného kamerového dohľadu na univerzite (*Antović a Mirković proti Čiernej Hore*, 2017, § 44-45),

i) informácie o zdaniteľných príjmoch a majetku veľkého počtu osôb, bez ohľadu na skutočnosť, že verejnosť mala k takýmto údajom za určitých podmienok prístup (*Satakunnan Markkinapörssi Oy a Satamedia Oy proti Fínsku* [VK], 2017, § 138),

j) údaje o narodení a opustení jednotlivca vrátane informácií potrebných na zistenie pravdy o dôležitom aspekte osobnej identity (*Gaskin proti Spojenému kráľovstvu*, 1989, § 39; *Odièvre proti Francúzsku* [VK], 2003, § 28-29),

k) údaje obsiahnuté v dohode o rozvode manželstva, ktoré obsahujú podrobnosti o rozdelení majetku manželov, starostlivosti a bydlisku maloletých detí, dohodu o

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

výživnom a prehľad majetku/príjmov žiadateľa (*Liebscher proti Rakúsku*, 2021, § 31 a 68).

Podľa článku 2 Dohovoru 108 „spracovanie údajov“ zahŕňa: „akúkoľvek operáciu alebo súbor operácií vykonávaných s osobnými údajmi, ako je zhromažďovanie, ukladanie, uchovávanie, zmena, vyhľadávanie, zverejňovanie, sprístupňovanie, vymazanie alebo zničenie, alebo vykonávanie logických a/alebo aritmetických operácií s takýmito údajmi“. Rozvoj technológií viedol k rozšíreniu typov operácií s osobnými údajmi, ktoré môžu predstavovať spracúvanie.

Spracúvanie osobných údajov predstavuje komplexnú koncepciu v právnych predpisoch EÚ, ako aj Rady Európy: „‚spracúvanie osobných údajov‘ [...] je operácia [...], napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia“ osobných údajov. V modernizovanom Dohovore č. 108 sa do tohto vymedzenia pojmu dopĺňa uchovávanie osobných údajov. Príklad: Zamestnávatelia získavajú a spracúvajú údaje o svojich zamestnancoch vrátane informácií týkajúcich sa miezd. Právnym základom pre zákonnosť tejto činnosti sú pracovné zmluvy. Zamestnávatelia musia zasielať údaje o mzdách svojich zamestnancov daňovému úradu. Toto zasielanie údajov je takisto „spracúvaním“ v zmysle tohto pojmu v modernizovanom Dohovore č. 108 a v GDPR. Právnym základom takéhoto poskytovania však nie sú pracovné zmluvy. Pre spracovateľské operácie, ktoré vedú k poskytovaniu údajov o mzdách od zamestnávateľa daňovému úradu, musí existovať dodatočný právny základ. Tento právny základ sa zvyčajne nachádza v ustanoveniach vnútroštátnych daňových predpisov. Bez takýchto ustanovení – a bez akéhokoľvek iného legitímneho dôvodu na spracúvanie – by bolo toto poskytnutie údajov nezákonným spracúvaním.[237]

ESĽP ako spracúvanie identifikoval tieto typické príklady:

[237] Agentúra Európskej únie pre základné práva a Rada Európy. Príručka o európskych právnych predpisoch v oblasti ochrany údajov. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021, s. 101 – 103.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

a) zhromažďovanie informácií o účastníkoch spojených s konkrétnou dynamickou IP adresou jednotlivca políciou od poskytovateľa internetu (*Benedik proti Slovensku*, 2018, § 108 - 109),

b) skutočnosť zhromažďovania a uchovávania verejných informácií o jednotlivcovi, napríklad o jeho politickej činnosti (*Rotaru proti Rumunsku* [VK], 2000),

c) zaradenie jednotlivca do národnej súdnej databázy páchateľov sexuálnych trestných činov (*Gardel proti Francúzsku*, 2009, § 58) a zber a uchovávanie odtlačkov prstov podozrivého (*M.K. proti Francúzsku*, 2013, § 29),

d) utajené nahrávanie hlasových vzoriek na policajnej stanici na účely trvalého uchovávania, ktoré sa má použiť na identifikáciu dotknutých osôb, a to procesom analýzy v kontexte iných osobných údajov (*P.G. a J.H. proti Spojenému kráľovstvu*, 2001, § 59-60),

e) filmovanie jednotlivca v policajnej vypočúvacej miestnosti kamerami nainštalovanými z bezpečnostných dôvodov a úplne viditeľnými, s trvalým zaznamenávaním záznamu a jeho zaradením do montáže na ďalšie použitie (*Perry proti Spojenému kráľovstvu*, 2003, § 41),

f) systematické zhromažďovanie a uchovávanie údajov z monitorovania GPS, ktoré poukazujú na miesto pobytu a pohyb subjektu na verejnosti (*Uzun proti Nemecku*, 2010, § 49-53),

g) uverejnenie článku v časopise ilustrovaného fotografiami známych osobností vyhotovenými bez ich vedomia [*Von Hannover proti Nemecku (č. 2)* [VK], 2012, § 95-99],

h) zaznamenanie a zverejnenie záznamu z priemyselnej kamery médiám, na ktorom sa jednotlivec pokúša spáchať samovraždu na verejnom mieste (*Peck proti Spojenému kráľovstvu*, 2003, § 59-63),

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

i) zaznamenávanie a uchovávanie údajov o údajnom zamestnaní jednotlivca políciou (*Khelili proti Švajčiarsku*, 2011, § 56),

j) poskytnutie veľmi citlivých dôverných informácií o súkromnom živote pacienta psychiatrickou nemocnicou novinárom *(Mockutė proti Litve*, 2018, § 99),

k) zhromažďovanie informácií štátom v rámci antidopingových opatrení v športe o mieste pobytu a každodenných aktivitách športovcov na vysokej úrovni, a to aj počas víkendov [*National Federation of Sportspersons' Associations and Unions (FNASS) a ostatní proti Francúzsku*, 2018, § 155-159],

l) systematické skenovanie a nahrávanie súkromnej korešpondencie väzňov, a to tak prichádzajúcej, ako aj odchádzajúcej, na server Národnej justičnej siete (*Nuh Uzun a ostatní proti Turecku*, 2022, § 80-82).

Takéto opatrenia ESĽP takmer vždy považuje za zásahy s rôznym stupňom závažnosti do práva na rešpektovanie súkromného života, obydlia alebo korešpondencie dotknutých osôb.

Nie všetky operácie s osobnými údajmi však patria do rozsahu pôsobnosti článku 8 alebo automaticky zasahujú do príslušných práv. Tak vo veci *Mehmedovic proti Švajčiarsku* (odm.), 2018 (§ 18) ESĽP zaujal stanovisko, že kusé informácie týkajúce sa sťažovateľky, ktoré boli zhromaždené náhodne a nemali žiadny význam pre predmetné vyšetrovanie, v žiadnom prípade nepredstavovali systematické alebo trvalé zhromažďovanie údajov, a teda nezasahovali do jej práva na rešpektovanie súkromného života. Okrem toho vo veci *Cakicisoy a ostatní proti Cypru* (odm.), 2014 (§ 50-52) sa skutočnosť, že orgány odobrali sťažovateľom vzorky krvi na získanie ich profilu DNA pre exhumačný program na identifikáciu pozostatkov ich zosnulých príbuzných a že vzorky boli zničené po uplynutí platnosti formulárov súhlasu, nepovažovala za zásah do práva sťažovateľov na rešpektovanie ich súkromného života.

ESĽP vo svojej rozhodovacej činnosti tiež na základe čl. 6 Dohovoru č. 108 vytvoril klasifikáciu osobných údajov a rozoznáva ich tzv. citlivé kategórie a tzv. ostatné kategórie.

Podľa článku 6 Dohovoru č. 108 sa osobné údaje odhaľujúce rasový pôvod, politické názory, náboženské alebo iné presvedčenie a informácie o zdraví alebo sexuálnom živote jednotlivca

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

alebo o akýchkoľvek odsúdeniach za trestné činy nemôžu spracúvať automaticky, pokiaľ vnútroštátne právo nestanovuje primerané záruky. Informácie patriace do týchto kategórií, ktoré ESĽP označil za „citlivé“, si podľa neho vyžadujú zvýšený stupeň ochrany. Zaraďuje medzi ne:

1) údaje odhaľujúce rasový alebo etnický pôvod,
2) údaje odhaľujúce politické názory a náboženské alebo iné presvedčenie vrátane filozofického,
3) údaje odhaľujúce členstvo v odboroch,
4) genetické a biometrické údaje,
5) údaje týkajúce sa zdravia, sexuálneho života alebo sexuálnej orientácie,[238]
6) údaje o trestných činoch a odsúdeniach.

Okrem údajov označených ako „citlivé“ sú významné aj ďalšie kategórie osobných údajov, najmä v súvislosti so stále sofistikovanejšími technikami dohľadu a schopnosťou informačných a komunikačných technológií sťažovať každodenný život dotknutých osôb. Medzi ne sa zaraďujú:

1) údaje o zamestnaní,
2) finančné údaje,
3) dopravné údaje,
4) hlasové vzorky,
5) údaje o polohe GPS,
6) fotografie.

[238] Zverejnenie takýchto údajov môže dramaticky ovplyvniť jeho súkromný a rodinný život, ako aj sociálnu a pracovnú situáciu tým, že ho vystaví jeho alebo jej opovrhnutiu a riziku ostrakizmu (*Z proti Fínsku*, 1997, § 96; *C.C. proti Španielsku*, 2009, § 33; *P. a S. proti Poľsku,* 2012, § 128; *Avilkina a ostatní proti Rusku*, 2013, § 45; *Y. proti Turecku* (odm.), 2015, § 65; *Y. G. proti Rusku,* 2022, § 45).

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

7.3 VŠEOBECNE K ROZHODOVACEJ ČINNOSTI SÚVISIACEJ SO ZAMESTNANECKÝMI VZŤAHMI

Zaznamenávanie údajov týkajúcich sa zamestnania o identifikovanej alebo identifikovateľnej osobe a ich uchovávanie predstavuje zásah do práva dotknutej osoby na rešpektovanie jej súkromného a rodinného života podľa článku 8 (*Khelili proti Švajčiarsku,* 2011, § 56; *Sõro proti Estónsku*, 2015, § 49 a 56).

Akékoľvek informácie totiž môžu byť osobnými údajmi za predpokladu, že sa týkajú identifikovanej alebo identifikovateľnej osoby. Príklad: Posudok pracovného výkonu zamestnanca zo strany nadriadeného, ktorý je uložený v osobnom spise zamestnanca, predstavuje osobné údaje o zamestnancovi. Platí to aj v prípade, keď čiastočne alebo úplne vyjadruje len osobný názor nadriadeného, napríklad: „zamestnanec neprejavuje pri práci nasadenie“ a neobsahuje faktické informácie, napríklad: „za posledných šesť mesiacov nebol zamestnanec päť týždňov prítomný na pracovisku“.[239]

Vzhľadom na to, že informácie zhromaždené orgánmi a uchovávané v ich evidencii sú v súčasnosti predmetom automatického spracovania, ktoré výrazne uľahčuje prístup k takýmto údajom a ich prenos, takéto opatrenia by mohli mať vážne dôsledky, ktoré by mohli poškodiť povesť jednotlivcov alebo sťažiť ich každodenný život. ESĽP konštatoval porušenie článku 8 vo veci *Khelili proti Švajčiarsku*, 2011 (§ 64), kde bola sťažovateľka zaznamenaná políciou ako „prostitútka“, pričom tento záznam bol následne v databáze opravený a nahradený záznamom „krajčírka“,[240] a aj vo veci *Sõro proti Estónsku*, 2015 (§ 63), kde bol sťažovateľ nútený odísť zo

[239] Agentúra Európskej únie pre základné práva a Rada Európy. Príručka o európskych právnych predpisoch v oblasti ochrany údajov. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021, s. 91.

[240] V danej veci polícia počas policajnej kontroly zistila, že sťažovateľka má pri sebe vizitky, na ktorých bolo napísané: „Milá a pekná žena pred štyridsiatkou by sa rada zoznámila s mužom, ktorý by s ňou občas zašiel na pohárik alebo do spoločnosti. Tel. č. [...].“ Sťažovateľka tvrdila, že po nájdení vizitiek polícia zapísala jej meno do registra prostitútok, čo je zamestnanie, ktoré ona trvale popiera. Sťažovateľka požadovala odstránenie slova „prostitútka“ z policajných počítačových záznamov. ESĽP v zásade uznal, že uchovávanie osobných údajov jednotlivca na základe skutočnosti, že táto osoba by mohla spáchať iný trestný čin, môže byť za určitých okolností primerané. V prípade sťažovateľky sa podozrenie z nezákonnej prostitúcie zdalo byť príliš neurčité a všeobecné, nebolo doložené konkrétnymi skutočnosťami, keďže sťažovateľka nikdy nebola odsúdená za nezákonnú prostitúciu, a teda nie je možné hovoriť o „naliehavej spoločenskej potrebe“ podľa článku 8 Dohovoru. ESĽP zohľadnil skutočnosť, že orgány mali overiť presnosť uchovávaných údajov o sťažovateľke, ako aj závažnosť zásahu do jej práv a skonštatoval, že dlhoročný zápis slova „prostitútka“ v policajných spisoch nebol nevyhnutný v demokratickej spoločnosti. Súd dospel k záveru, že došlo k porušeniu článku 8 Dohovoru;

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zamestnania po zverejnení údajov o svojom zamestnaní ako vodiča pre bývalé bezpečnostné služby.

Hoci základným cieľom článku 8 Dohovoru je chrániť jednotlivcov pred svojvoľným zásahom zo strany orgánov verejnej moci alebo súkromných subjektov, ktorým bola zverená rozhodovacia právomoc delegovaná štátom, do ich práva na rešpektovanie súkromného a rodinného života, domova a korešpondencie, môže tiež tento článok uložiť štátu určité pozitívne povinnosti na zabezpečenie účinného dodržiavania týchto práv (*Bărbulescu proti Rumunsku* [VK], 2017, § 108).

Vo veci *Vukota-Bojić proti Švajčiarsku,* 2016 (§ 47) ESĽP zdôraznil, že štát sa nemôže zbaviť zodpovednosti podľa Dohovoru tým, že deleguje svoje povinnosti na súkromné orgány alebo jednotlivcov. Vzhľadom na to, že súkromná poisťovňa, ktorá zhromažďovala a uchovávala osobné údaje, prevádzkovala štátny systém poistenia a že ju vnútroštátny režim považoval za orgán verejnej moci, spoločnosť sa musela považovať za orgán verejnej moci a činy, ktoré spáchala, boli pričítateľné žalovanému štátu (tamže, § 47).

Vo veci *Libert proti Francúzsk*u, 2018 (§ 37-41) ESĽP zamietol námietku vlády že Národnú železničnú spoločnosť (SNCF), zamestnávateľa sťažovateľa, ktorý bol obvinený z otvárania osobných súborov na pracovnom počítači, nemožno považovať za orgán verejnej moci na účely článku 8. Aj keď jej zamestnanci boli zamestnaní podľa súkromného práva, spoločnosť bola verejnoprávny subjekt, ktorý podliehal štátnemu dohľadu a mal štátom vymenovaných riaditeľov, a teda spoločnosť požívala implicitnú štátnu záruku.

Pokiaľ ide o menej závažné úkony vykonané jednotlivcami, ako je monitorovanie zamestnancov na pracovisku, štáty si môžu vybrať, či prijmú osobitné právne predpisy týkajúce sa videodohľadu alebo nie (*López Ribalda a ostatní proti Španielsku* [VK], 2019, § 113; *Köpke proti Nemecku* (odm.), 2010) alebo monitorovanie korešpondencie nesúvisiacej s výkonom profesie (*Bărbulescu proti Rumunsku* [VK], 2017, § 119). Napriek tomu je na vnútroštátnych súdoch, aby zabezpečili, že akákoľvek implementácia opatrení dohľadu zamestnávateľa, ktoré

Agentúra Európskej únie pre základné práva a Rada Európy. Príručka o európskych právnych predpisoch v oblasti ochrany údajov. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021, s. 43.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zasahujú do práva zamestnancov na rešpektovanie ich súkromného života alebo korešpondencie, bola primeraná a sprevádzaná vhodnými a primeranými zárukami proti zneužívaniu [*Köpke proti Nemecku* (odm.), 2010; *Bărbulescu proti Rumunsku* [VK], 2017, § 120; *López Ribalda a ostatní proti Španielsku* [VK], 2019, § 116).

V článku 8 ods. 2 Dohovoru sa uvádzajú podmienky, za ktorých môže dôjsť k zásahu do výkonu chráneného práva; takýto zásah musí byť „v súlade so zákonom“, musí sledovať „legitímny cieľ“ a musí byť „nevyhnutný v demokratickej spoločnosti“.

1. podmienka – či bol zásah zákonný. ESĽP vo viacerých prípadoch skúmal otázku, či bola alebo nebola splnená požiadavka uvedená v článku 5 Dohovoru č. 108, že osobné údaje podliehajúce automatickému spracovaniu musia byť získané a spracované spravodlivo a zákonne. V mnohých prípadoch ESĽP zistil porušenie článku 8 výlučne už z dôvodu nedostatku právneho základu na vnútroštátnej úrovni, ktorý by povolil opatrenia, ktoré by mohli zasahovať do príslušných práv (*Taylor-Sabori proti Spojenému kráľovstvu*, 2002, § § 17 – 19, *Radu proti Moldavsku*, 2014, § 31, *Mockutė proti Litve*, 2018, § 103 – 104, *M. D. a ostatní proti Španielsku*, 2022, § 61 – 64).

2. podmienka – či zásah sledoval legitímny cieľ. Vo veci *López Ribalda a ostatní proti Španielsku* [VK], 2019 (§ 118 a 123) mohol legitímny záujem zamestnávateľa na prijatí opatrení s cieľom zistiť a potrestať osobu(y) zodpovednú(é) za podozrenie z krádeže s cieľom zabezpečiť ochranu majetku spoločnosti a jej plynulý chod odôvodniť opatrenia zahŕňajúce kamerový dohľad nad zamestnancami na pracovisku.

3. podmienka – či bol zásah „nevyhnutný v demokratickej spoločnosti“. V súvislosti s obzvlášť závažnými činmi medzi jednotlivcami, ktoré môžu zasiahnuť do práv podľa článku 8, sa preskúmanie ESĽP, či tieto spĺňajú požiadavku „nevyhnutnosti v demokratickej spoločnosti“, týka spôsobu, akým štát prijal osobitné právne predpisy na zabezpečenie dostatočnej ochrany týchto práv (*K.U. proti Fínsku*, 2008, § 43-50; *Söderman proti Švédsku* [VK], 2013, § 80-83). Pokiaľ ide o menej závažné úkony medzi jednotlivcami, ako je napríklad kamerové sledovanie zamestnancov na pracovisku, preskúmanie ESĽP, či bolo opatrenie „nevyhnutné v demokratickej spoločnosti“, sa bude týkať spôsobu, akým vnútroštátne súdy zohľadnili

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

kritériá, ktoré ESĽP ustanovil vo svojej judikatúre, čím sa preukáže, či boli konkurenčné záujmy zvážené (proporčné) (*López Ribalda a ostatní proti Španielsku* [VK], 2019, § 116-117, § 122). Pri preskúmaní týchto kritérií, ak sa zistí, že jedno z nich chýba, záruky vyplývajúce z ostatných budú o to dôležitejšie a môžu dostatočne kompenzovať toto zlyhanie (ibid., § 131).

7.3.1 Operácie s údajmi, ktoré môžu porušiť právo na rešpektovanie súkromného života – zhromažďovanie osobných údajov

S rozvojom technológií získava zber, uchovávanie a zverejňovanie údajov širokú škálu foriem. V niekoľkých prípadoch ESĽP posudzoval, či jedna alebo viaceré z týchto operácií neviedli k neoprávnenému zásahu do práva dotknutej osoby na rešpektovanie jej súkromného života.

ESĽP skúmal operácie zhromažďovania osobných údajov v rôznych kontextoch: pokiaľ ide o akcie na boj proti organizovanému zločinu a terorizmu prostredníctvom rôznych tajných sledovacích systémov vytvorených orgánmi; v súdnom kontexte týkajúcom sa osobných údajov, ktoré orgány zhromažďujú na účely použitia pri dokazovaní; v kontexte zdravotníctva; v kontexte údajov zhromažďovaných na pracovisku, ktoré sa vzťahujú na zamestnávateľov vo verejnom aj súkromnom sektore; a napokon v kontexte zákonných povinností verejných alebo súkromných orgánov poskytnúť orgánom osobné údaje, ktoré majú k dispozícii, na ochranu všeobecného verejného záujmu.

7.3.1.1 Zber údajov zamestnávateľmi na pracovisku

ESĽP posudzoval podľa článku 8 Dohovoru otázku zhromažďovania osobných údajov na pracovisku zamestnávateľmi vo verejnom sektore (*Halford proti Spojenému kráľovstvu*, 1997, § 49, 45; *Antović a* Mirković *proti Čiernej Hore*, 2017, § 58; *Libert proti Francúzsku*, 2018, § 41) alebo v súkromnom sektore (*Köpke proti Nemecku* (odm.), 2010; *Bărbulescu proti Rumunsku* [VK], 2017, § 109; a *López Ribalda a ostatní proti Španielsku* [VK], 2019, § 109). V niektorých prípadoch sa operácia zhromažďovania údajov uskutočnila bez vedomia dotknutých osôb, a to prostredníctvom sledovania, ktoré bolo buď úplne utajené (*Halford proti Spojenému kráľovstvu*, 1997, § 49; *Copland proti Spojenému kráľovstvu*, 2007, § 45; *Bărbulescu proti Rumunsku* [VK], 2017, § 78), alebo čiastočne (*López Ribalda a ostatní proti Španielsku* [VK],

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

2019, § 93), zatiaľ čo v iných prípadoch boli údaje zhromažďované s plným vedomím dotknutých zamestnancov (*Antović a Mirković proti Čiernej Hore*, 2017, § 44).

Osobné údaje, ktoré sa mali zhromažďovať, mali pôvod v: sledovaní neprofesionálnych telefonických hovorov[241] z pracovných priestorov (*Halford proti Spojenému kráľovstvu*, 1997, § 44); monitorovaní používania telefónu, e-mailu a internetu na pracovisku (*Copland proti Spojenému kráľovstvu*, 2007, § 44-49); monitorovaní používania internetu a okamžitých správ (Yahoo) (*Bărbulescu proti Rumunsku* [VK], 2017, § 74); otváraní súborov uložených zamestnancom na počítači poskytnutom jeho zamestnávateľom na pracovné účely (*Libert proti Francúzsku*, 2018, § 25); alebo fotografiách vyhotovených prostredníctvom videozáznamu, na ktorých je zachytené správanie identifikovaného alebo identifikovateľného zamestnanca na jeho pracovisku (*Köpke proti Nemecku* (odm.), 2010; *Antović a Mirković proti Čiernej Hore*, 2017, § 44; *López Ribalda a ostatní proti Španielsku* [VK], 2019, § 92).

V prvých dvoch rozsudkoch vydaných v tejto oblasti (*Halford proti Spojenému kráľovstvu,* 1997, § 44, a Copland *proti Spojenému kráľovstvu*, 2007, § 41) ESĽP rozhodol, že neslužobné telefonické hovory z obchodných priestorov sú *prima facie* zahrnuté pod pojmy „súkromný život“ a „korešpondencia“ na účely článku 8. Taktiež sa domnieval, že e-maily odoslané z práce by mali byť podobne chránené podľa článku 8, rovnako ako informácie získané z monitorovania používania internetu (*Copland proti Spojenému kráľovstvu*, 2007, § 41).[242] Následne ESĽP tiež spresnil, že pod pojem „súkromný život“ môžu spadať aj údaje jasne

[241] Vo význame nesúvisiacich so zamestnaním – pozn. autora, neslužobných. V rovnakom význame pozri aj ďalšom texte.

[242] Bežným problémom v oblasti ochrany údajov v súčasnom bežnom pracovnom prostredí je rozsah legitímneho monitorovania elektronických komunikácií zamestnancov na pracovisku. Často sa tvrdí, že tento problém možno jednoducho vyriešiť zákazom súkromného používania služobných komunikačných prostriedkov. Takýto všeobecný zákaz by však bol neprimeraný a nereálny. V tejto súvislosti majú osobitný význam rozsudky ESĽP vo veciach *Copland proti Spojenému kráľovstvu* a *Bărbulescu proti Rumunsku*. Príklad: Vo veci *Copland proti Spojenému kráľovstvu* išlo o tajné monitorovanie používania služobného telefónu, elektronickej pošty a internetu zamestnankyňou vysokej školy s cieľom potvrdiť, či skutočne neprimerane používa služobné prostriedky na osobné účely. ESĽP konštatoval, že telefonické hovory z pracovných priestorov patria do rozsahu pojmov súkromný život a korešpondencia. Preto sú takéto hovory a e-maily zaslané zo zamestnania, ako aj informácie získané na základe monitorovania súkromného využívania internetu chránené článkom 8 Dohovoru. V prípade sťažovateľky neexistovali žiadne ustanovenia, ktorými by sa upravovali podmienky, za ktorých by zamestnávatelia mohli monitorovať používanie telefónu, e-mailu a internetu zamestnancami. Zásah teda nebol v súlade s právnymi predpismi. ESĽP dospel k záveru, že došlo k porušeniu článku 8 Dohovoru; Agentúra Európskej únie pre základné práva a Rada Európy. Príručka o európskych právnych predpisoch v oblasti ochrany údajov. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021, s. 344 a nasl.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

označené ako súkromné a uložené zamestnancom v počítači, ktorý mu poskytol jeho zamestnávateľ na pracovné účely (*Libert proti Francúzsku*, 2018, § 25). Okrem toho, utajené vyhotovovanie videozáznamu, na ktorom je zachytené správanie zamestnanca na pracovisku bez oznámenia, tiež ovplyvňuje jeho „súkromný život“ [*Köpke proti Nemecku* (odm.), 2010]. Následne ESĽP nevidel dôvod, prečo by sa mal od tohto záveru odchýliť bez ohľadu na to, či je videozáznam zamestnancov na ich pracovisku vyhotovený utajene alebo nie (*Antović a Mirković proti Čiernej Hore*, 2017, § 44; *López Ribalda a ďalší proti Španielsku* [VK], 2019, § 93).

Vo veciach *Halford proti Spojenému kráľovstvu*, 1997 (§ 50-51) a *Copland proti Spojenému kráľovstvu*, 2007 (§ 48) ESĽP konštatoval, že vzhľadom na to, že v rozhodnom čase neexistovalo vnútroštátne ustanovenie, ktoré by povoľovalo zhromažďovanie osobných údajov z neslužobných telefonických hovorov zamestnancov, resp. z elektronických správ odoslaných z pracoviska, výsledný zásah do ich práva na rešpektovanie súkromného života nebol „v súlade so zákonom“. Vo veci *Köpke proti Nemecku* (odm.), 2010, ESĽP vyhlásil za zjavne neopodstatnenú sťažnosť na zamestnávateľa, ktorý za pomoci súkromnej detektívnej agentúry zhromažďoval údaje o pokladníčke supermarketu podozrivej z krádeže pomocou utajeného vyhotovenia videozáznamu. Aj keď v čase rozhodovania vo veci samej podmienky, za ktorých môže zamestnávateľ pristúpiť k sledovaniu zamestnanca prostredníctvom videozáznamu, ešte neboli ustanovené v právnych predpisoch, judikatúra Spolkového pracovného súdu ustanovila hlavné záruky proti svojvoľnému zasahovaniu do práva zamestnancov na rešpektovanie ich súkromného života.

Existencia dôvodného podozrenia, že došlo k závažnému porušeniu pracovnej disciplíny, a rozsah strát zistených v tomto prípade môžu predstavovať závažné odôvodnenie pre zamestnávateľa, aby zaviedol zber osobných údajov na pracovisku (*López Ribalda a ostatní proti Španielsku* [VK], 2019, § 134). Naopak, samotné podozrenie zo sprenevery alebo iného protiprávneho konania zo strany zamestnancov nemôže odôvodniť inštaláciu utajeného monitorovania videozáznamom zo strany zamestnávateľa (tamže, § 134).

Vo veci *Bărbulescu proti Rumunsku* [VK], 2017 (§ 121) ESĽP definoval niekoľko kritérií, ktoré musia byť splnené v súvislosti s opatreniami zameranými na dohľad nad korešpondenciou a

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

komunikáciou zamestnancov na ich pracovisku, ak nemajú byť v rozpore s článkom 8. V tejto súvislosti musia vnútroštátne orgány odpovedať na tieto otázky: Bol zamestnanec informovaný o možnosti, že zamestnávateľ môže prijať opatrenia na kontrolu korešpondencie a inej komunikácie, a o vykonávaní takýchto opatrení? Aký bol rozsah monitorovania zo strany zamestnávateľa a miera zásahu do súkromia zamestnanca? Uviedol zamestnávateľ legitímne dôvody, ktorými odôvodnil monitorovanie komunikácie zamestnanca? Bolo by možné vytvoriť systém monitorovania založený na menej rušivých metódach a opatreniach, než je priamy prístup k obsahu komunikácie zamestnanca? Aké boli dôsledky monitorovania pre zamestnanca, ktorý mu bol vystavený? Boli zamestnancovi poskytnuté primerané záruky, najmä ak monitorovacie operácie zamestnávateľa mali rušivý charakter? A napokon, vnútroštátne orgány by mali zabezpečiť, aby zamestnanec, ktorého komunikácia bola monitorovaná, mal prístup k opravnému prostriedku pred súdnym orgánom s právomocou určiť, aspoň v podstate, ako boli dodržané vyššie uvedené kritériá a či boli napadnuté opatrenia zákonné (tamže, § 122).

Následne vo veci *López Ribalda a ostatní proti Španielsku* [VK], 2019 (§ 116) ESĽP poukázal na to, že tieto kritériá možno preniesť aj na opatrenia videodohľadu zavedené zamestnávateľom na pracovisku.

ESĽP konštatoval porušenie článku 8 v prípadoch, keď zistil, že vnútroštátne súdy nezabezpečili, aby bolo zavedenie opatrení dohľadu zo strany zamestnávateľa primerané a sprevádzané primeranými a dostatočnými zárukami. Vo veci *Bărbulescu proti Rumunsku* [VK], 2017 (§ 108-141) vnútroštátne súdy neurčili konkrétne dôvody odôvodňujúce vykonanie opatrení dohľadu, či sa zamestnávateľ mohol uchýliť k menej rušivým opatreniam vo vzťahu k súkromnému životu a korešpondencii zamestnanca, alebo či bol zamestnanec vopred upozornený svojim zamestnávateľom o možnom monitorovaní jeho komunikácie. Naopak, vo veci *Libert proti Francúzsku*, 2018 (§ 37-53) ESĽP nezistil žiadne porušenie článku 8 týkajúce sa otvorenia osobných súborov uložených v pracovnom počítači, ktorých pornografický obsah bol dôvodom na prepustenie zamestnanca. Poznamenal, že vnútroštátne právo, ako ho vykladal a uplatňoval vnútroštátny súd, obsahovalo primerané záruky proti svojvôli vrátane

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

skutočnosti, že zamestnávateľ mohol otvoriť súbory označené ako „osobné“ len v prítomnosti zamestnanca.

Podľa názoru ESĽP len naliehavá požiadavka týkajúca sa ochrany významných verejných alebo súkromných záujmov mohla odôvodniť, že zamestnávateľ vopred neinformoval zamestnancov o opatreniach, ktoré by mohli narušiť ochranu osobných údajov zamestnancov (*López Ribalda a ostatní proti Španielsku* [VK], 2019, § 133). Pred zavedením opatrení na zber ich údajov by mal zamestnávateľ informovať dotknutých zamestnancov o existencii a podmienkach takéhoto zberu údajov, aj keď len všeobecným spôsobom (tamže, § 131). Požiadavka transparentnosti a z nej vyplývajúce právo na informácie majú zásadný význam najmä v kontexte pracovnoprávnych vzťahov, kde má zamestnávateľ významné právomoci vo vzťahu k zamestnancom, a je potrebné zabrániť akémukoľvek zneužitiu týchto právomocí. Poskytovanie informácií sledovanej osobe a ich rozsah však predstavujú len jedno z kritérií, ktoré treba zohľadniť pri posudzovaní primeranosti opatrenia tohto druhu v konkrétnom prípade. Ak však takéto informácie chýbajú, záruky vyplývajúce z ostatných kritérií budú o to dôležitejšie (tamže, § 131).

Ak neboli poskytnuté žiadne predchádzajúce informácie, je dôležité zistiť, či zamestnanci, ktorí boli podrobení sledovaniu, mali k dispozícii vnútroštátne prostriedky nápravy osobitne určené na zabezpečenie účinnej ochrany práva na rešpektovanie súkromného života. V rámci opatrení uložených zamestnancom na pracovisku možno takúto ochranu zabezpečiť rôznymi prostriedkami, ktoré môžu patriť do pracovného práva, ale aj do občianskeho, správneho alebo trestného práva (tamže, § 136).

Konkrétnejšie v súvislosti s videodohľadom zamestnancov poukázal ESĽP vo veci *López Ribalda a ostatní proti Španielsku* [VK], 2019 (§ 125) na to, že pri analýze primeranosti opatrenia videodohľadu je potrebné rozlišovať medzi rôznymi miestami, na ktorých sa monitorovanie vykonávalo, a to z hľadiska ochrany súkromia, ktorú by zamestnanec mohol odôvodnene očakávať. Toto očakávanie je veľmi vysoké na miestach, ktoré sú svojou povahou súkromné, ako sú toalety alebo šatne, kde je odôvodnená zvýšená ochrana alebo dokonca úplný zákaz monitorovania videozáznamom (tamže, § 125, 61, 65, s odkazom na príslušné medzinárodné dokumenty). Zostáva vysoká v uzavretých pracovných priestoroch, ako sú kancelárie, a je

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zjavne nižšia na miestach, ktoré sú viditeľné alebo prístupné kolegom alebo širokej verejnosti (ibid., § 125).

V tejto súvislosti vo veci *Köpke proti Nemecku* (odm.), 2010, ESĽP vyhlásil za neprijateľnú ako zjavne nepodloženú sťažnosť podanú sťažovateľkou, pokladníčkou v supermarkete, týkajúcu sa utajeného kamerového dohľadu, ktorý jej zamestnávateľ vykonával s pomocou súkromnej detektívnej agentúry. ESĽP najmä uviedol, že napadnuté opatrenie bolo časovo obmedzené (dva týždne) a vzťahovalo sa len na priestor prístupný verejnosti v okolí pokladní, že získané videozáznamy spracúval obmedzený počet osôb pracujúcich pre detektívnu agentúru a zamestnancov zamestnávateľa a že boli použité výlučne v rámci konania o prepustení žalobkyne a konania pred pracovným súdom.

Naopak, v rozsudku vo veci *Antović a Mirković proti Čiernej Hore,* 2017 (§ 55-60) ESĽP konštatoval porušenie článku 8 z dôvodu, že údajný zásah do súkromného života sťažovateľov, dvoch univerzitných profesorov, v dôsledku inštalácie kamerového systému v univerzitných posluchárňach, v ktorých mali výučbu, nebol ustanovený v súlade so zákonom.

Vo veci *López Ribalda a ostatní proti Španielsku* [VK], 2019 (§ 137) ESĽP nezistil porušenie článku 8 v súvislosti s čiastočne otvoreným a čiastočne utajeným kamerovým sledovaním pokladní a predavačov v supermarkete, okrem iného so zreteľom na podstatné záruky stanovené španielskou legislatívou vrátane opravných prostriedkov, ktoré sťažovatelia nevyužili.

7.3.1.2 Uchovávanie osobných údajov

Uchovávanie informácií o súkromnom živote jednotlivca orgánom verejnej moci, bez ohľadu na to, aké informácie sa získavajú, predstavuje zásah do práva na rešpektovanie súkromného života dotknutej osoby podľa článku 8 Dohovoru, či už sa údaje následne použijú alebo nie (*Ammán proti Švajčiarsku* [VK], 2000, § 69; *Rotaru proti Rumunsku* [VK], 2000, § 46; *S. a Marper proti Spojenému kráľovstvu* [VK], 2008, § 67). Skutočne súkromný charakter týchto informácií si vyžaduje, aby ESĽP dôkladne preskúmal akékoľvek štátne opatrenie, ktoré povoľuje ich uchovávanie a používanie orgánmi bez súhlasu dotknutej osoby (*S. a Marper v. Spojené kráľovstvo* [VK], 2008, § 104).

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Prípad *M.M. proti Spojenému kráľovstvu* z roku 2012 sa týkal dôsledkov zmien politiky o dobe uchovávania osobných údajov v registri trestov z hľadiska vyhliadok dotknutej osoby na zamestnanie (§ 204). ESĽP sa domnieval, že nediskriminačné a neobmedzené zhromažďovanie údajov z registra trestov pravdepodobne nebude v súlade s požiadavkami článku 8, ak neexistujú jasné a podrobné zákonné predpisy objasňujúce uplatniteľné záruky a stanovujúce pravidlá upravujúce, okrem iného, trvanie o uchovávaní týchto údajov (tamže, § 199).

7.3.1.3 Zverejnenie osobných údajov

V niekoľkých prípadoch ESĽP posúdil opatrenia, ktoré zahŕňajú sprístupnenie osobných údajov jednotlivca sprostredkovateľom údajov, t. j. inej fyzickej alebo právnickej osobe (*Mockutė proti Litve*, 2018, § 99-100 - prípad týkajúci sa prenosu informácií o zdravotnom stave pacienta nemocnicou členovi jej rodiny a novinárom; *Radu proti Moldavskej republike*, 2014, § 27 - prípad týkajúci sa sprístupnenia lekárskych informácií o pacientovi zamestnávateľovi; *M.C. proti Spojenému kráľovstvu*, 2021, § 46 - prípad týkajúci sa sprístupnenia informácií o registri trestov žalobkyne zo strany orgánov jej potenciálnemu zamestnávateľovi).

Vo veci *Y. proti Turecku* (odm.), 2015, § 70-72, išlo o prípad týkajúci sa sprístupnenia informácií o HIV pozitívnom stave pacienta posádkou rýchlej lekárskej pomoci personálu nemocnice – sťažovateľ bol HIV pozitívny. Keďže bol počas svojho príchodu do nemocnice v bezvedomí, posádka sanitky informovala pracovníkov nemocnice, že je HIV pozitívny. Sťažovateľ pred ESĽP tvrdil, že zverejnenie týchto informácií porušilo jeho právo na rešpektovanie súkromného života. Vzhľadom na potrebu zaručiť bezpečnosť zamestnancov nemocnice sa však poskytnutie tejto informácie nepovažovalo za porušenie jeho práv. ESĽP tak vychádzal zo znenia čl. 8 ods. 2 Dohovoru, kde „ochrana práv a slobôd iných“ sa uvádza ako jeden z legitímnych dôvodov na obmedzenie práva na ochranu údajov.[243]

Vo veci *I proti Fínsku*, 2008, sťažovateľka nebola schopná dokázať, že jej zdravotné záznamy boli nezákonne sprístupnené ďalším zamestnancom nemocnice, v ktorej pracovala. Vnútroštátne súdy preto zamietli jej sťažnosť na porušenie práva na ochranu údajov. ESĽP

[243] Agentúra Európskej únie pre základné práva a Rada Európy. Príručka o európskych právnych predpisoch v oblasti ochrany údajov. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021, s. 165.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

dospel k záveru, že došlo k porušeniu článku 8 Dohovoru, keďže systém registrácie zdravotných záznamov v nemocnici „bol taký, že nebolo možné spätne vyjasniť používanie záznamov o pacientoch, keďže v systéme sa zobrazovalo len päť posledných nahliadnutí a tieto informácie boli odstránené po vrátení spisu do archívu“. Pre súd bolo rozhodujúce, že systém zavedený v nemocnici zjavne nebol v súlade s právnymi požiadavkami obsiahnutými vo vnútroštátnych právnych predpisoch, a vnútroštátne súdy túto skutočnosť náležite nezohľadnili.[244]

7.3.1.4 Vplyv predchádzajúceho súhlasu

Skutočnosť, že osobné údaje jednotlivcov sa zverejňujú na ich žiadosť alebo s ich súhlasom, ich ešte nezbavuje ochrany poskytovanej článkom 8, ak nemajú jednotlivci skutočnú možnosť výberu, napríklad ak zamestnávateľ trvá na poskytnutí osobných údajov uložených na zázname v registri trestov uchádzača o zamestnanie (*M.M. proti Spojenému kráľovstvu*, 2012, § 189). V danom prípade sťažovateľka požiadala o sprístupnenie informácií potenciálnemu zamestnávateľovi o záznamoch v jej registri trestov. ESĽP konštatoval porušenie článku 8 z dôvodu nedostatku dostatočných záruk v systéme uchovávania a zverejňovania údajov z registra trestov, ktoré v žiadnom štádiu neposkytovali posúdenie prípustnej relevantnosti údajov pre požadované zamestnanie alebo rozsahu, v akom by dotknutá osoba mohla predstavovať pretrvávajúce riziko (tamže, § 204). V *M.C. proti Spojenému kráľovstvu*, 2021, § 47 – 57, ESĽP zaznamenal legislatívne zmeny zavedené po *M. M. proti Spojenému kráľovstvu* a zistil, že novozavedený režim zverejňovania informácií o registri trestov je zlučiteľný s príslušnými požiadavkami článku 8: rozlišuje medzi rôznymi typmi trestných činov rôznymi spôsobmi; poskytuje istotu o tom, aké predchádzajúce odsúdenia budú kedykoľvek zverejnené; a stanovili vymedzené, obmedzené časové obdobie zverejnenia, ktoré by sa líšilo v závislosti od veku páchateľa a vnímanej závažnosti trestného činu.

Vo vzťahu k sprístupňovaniu údajov na ochranu verejného zdravia ESĽP uviedol, že právo osoby na rešpektovanie lekárskeho tajomstva nie je absolútne a musí sa posudzovať vo vzťahu k iným oprávneným právam a záujmom, ako je právo zamestnávateľa na kontradiktórne

[244] Tamže, s. 174 – 175.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

konanie (*Eternit proti Francúzsku* (odm.), 2012, § 37). Toto právo môže byť prevážené potrebou chrániť základný aspekt verejného záujmu, akým je bezpečnosť nemocničného personálu a ochrana verejného zdravia (*Y. v. Turecko* (odm.), 2015, § 74).

Vo vzťahu k zverejňovaniu údajov na ochranu národnej bezpečnosti ESĽP vo veci *Sõro proti Estónsku*, 2015 (§ 56-64) uviedol, že zverejnenie informácií v tom zmysle, že sťažovateľ bol zamestnaný ako šofér v bývalých bezpečnostných službách, predstavovalo porušenie článku 8, hoci žalobca bol vopred informovaný o zverejnení údajov a mohol napadnúť prenos údajov, nebol zavedený postup na posúdenie konkrétnych úloh vykonávaných jednotlivými zamestnancami bývalých bezpečnostných služieb s cieľom rozlíšiť nebezpečenstvo, ktoré by mohli predstavovať v demokratickom systéme niekoľko rokov po ukončení kariéry v týchto inštitúciách (tamže, § 61). ESĽP rozhodol, že akákoľvek hrozba, ktorú mohol sťažovateľ pôvodne predstavovať pre novovytvorenú demokraciu, sa musela s odstupom času medzi obnovením nezávislosti v Estónsku a zverejnením osobných údajov značne znížiť (tamže, § 62). Napriek tomu, že zákon o zverejňovaní informácií sám osebe neukladal žiadne obmedzenia pre sťažovateľov nový pracovný pomer, bol nútený odstúpiť zo svojho zamestnania vzhľadom na postoj jeho kolegov, ktorý nasvedčoval závažnosti zásahu do práva sťažovateľa na rešpektovanie jeho súkromného života (tamže, § 63).

7.3.2 Ochrana osobných údajov v kontexte práva na spravodlivý proces

Právo na spravodlivý proces je chránené čl. 6 ods. 1 Dohovoru. Podľa tohto ustanovenia má každý právo na to, aby jeho vec bola spravodlivo, verejne a v primeranej lehote prejednaná nezávislým a nestranným súdom zriadeným zákonom, ktorý rozhodne o jeho občianskych právach alebo záväzkoch alebo o akomkoľvek trestnom čine, z ktorého je obvinený. Rozsudok musí byť vyhlásený verejne, ale tlač a verejnosť môžu byť vylúčené buď po dobu celého alebo časti procesu v záujme mravnosti, verejného poriadku alebo národnej bezpečnosti v demokratickej spoločnosti, keď to vyžadujú záujmy maloletých alebo ochrana súkromného života účastníkov alebo, v rozsahu považovanom súdom za úplne nevyhnutný, pokiaľ by vzhľadom na osobitné okolnosti mohla byť verejnosť konania na ujmu záujmom spravodlivosti.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Každý jednotlivec, ktorého osobné údaje podliehajú automatickému spracovaniu v kontexte súdneho konania, musí požívať záruky článku 6, bez ohľadu na jeho postavenie v konaní (navrhovateľ, odporca, svedok, obvinený alebo tretia strana).

Všeobecné záruky práva na spravodlivý proces sú zakomponované v čl. 6 ods. 1 Dohovoru. V niekoľkých prípadoch ESĽP posudzoval z hľadiska článku 6 ods. 1 potrebu ochrany osobných údajov strán alebo tretích osôb v kontexte rôznych všeobecných záruk určených na zabezpečenie spravodlivosti súdneho konania. Ide najmä o rovnosť zbraní a právo na kontradiktórne konanie, právo na verejné prejednanie veci a verejné vyhlásenie rozsudku, dokazovanie, primeranú dĺžku konania a požiadavku na odôvodnenie súdnych rozhodnutí.

7.3.2.1 Rovnosť zbraní a rešpektovanie zásady kontradiktórnosti v konaniach týkajúcich sa citlivých alebo dôverných informácií

V prípade *Eternit proti Francúzsku* (odm.), 2012 (§ 35-42), zamestnávateľ podal žalobu proti rozhodnutiu zdravotnej poisťovne o uznaní povahy choroby ako choroby z povolania jedného zo svojich zamestnancov. ESĽP nezistil, že konanie bolo v rozpore s článkom 6 ods. 1 napriek tomu, že zamestnávateľovi nebola poskytnutá kópia vyjadrenia lekárskeho poradcu poisťovne. Neposkytnutie zdravotnej dokumentácie zamestnanca zamestnávateľovi bolo odôvodnené potrebou chrániť dôvernosť jeho zdravotných údajov, ktorú súdy museli zrovnoprávniť s právom sťažujúcej sa spoločnosti na kontradiktórne konanie, aby sa zabezpečilo, že samotná podstata práva nebola porušená ani v jednom prípade. Požadovaná rovnováha bola dosiahnutá v tom, že zamestnávateľ mohol požiadať súd, aby vymenoval nezávislého lekárskeho znalca, ktorý preskúma zdravotnú dokumentáciu zamestnanca a vypracuje správu – rešpektujúc dôvernosť zdravotnej dokumentácie – ako usmernenie súdu a účastníkov konania (tamže, § 37). Skutočnosť, že znalecký posudok nebol zadaný vždy, keď oň zamestnávateľ požiadal, ale len vtedy, keď súd usúdil, že nemá dostatočné informácie, nebola v rozpore s požiadavkami spravodlivého procesu podľa článku 6 ods. 1 Dohovoru (ibid., § § 35-39).

7.3.2.2 Zdôvodňovanie súdnych rozhodnutí a ochrana údajov

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

V prípade *Surikov proti Ukrajine*, 2017 (§ 102-103), ESĽP zistil porušenie článku 6 ods. 1 na základe toho, že vnútroštátne súdy sa nezaoberali množstvom relevantných a dôležitých žalobných bodov, ktoré boli nastolené. Sťažovateľ tvrdil, že jeho zamestnávateľ svojvoľne zhromažďoval a uchovával citlivé a neaktuálne informácie týkajúce sa jeho duševného zdravia, tieto informácie použil pri skúmaní jeho žiadosti o povýšenie a nezákonne ich poskytol jeho kolegom a súdu. Súd opätovne potvrdil, že článok 6 zaväzuje súdy, aby odôvodnili svoje rozsudky. Hoci túto povinnosť nemožno chápať tak, že vyžaduje podrobnú odpoveď na každý argument, zásada spravodlivosti by bola narušená, ak by vnútroštátne súdy ignorovali konkrétny, relevantný a dôležitý bod sťažovateľa (tamže, § 101 a judikatúra tam citované).

7.3.2.3 Použitie osobných údajov zhromaždených nezákonne alebo v rozpore s článkom 8 Dohovoru ako dôkazu

Otázkou použitia osobných údajov zhromaždených spôsobom, ktorý je v rozpore s požiadavkami vnútroštátneho práva alebo s požiadavkami článku 8 v súdnom konaní ako fyzického dôkazu, sa ESĽP zaoberal v niekoľkých prípadoch v kontexte správnych konaní (*Vukota-Bojic proti Švajčiarsku*, 2016, § 77 - o použití informácií tajne zhromaždených poisťovňou v rámci jej právomocí v rámci systému verejného poistenia v spore s poistencom); občianskoprávnych konaní (*Bărbulescu proti Rumunsku* [VK], 2017, § 140 – 141 - o používaní údajov zhromaždených zamestnávateľom o používaní internetu zamestnanca na pracovisku na účely odôvodnenia jeho prepustenia); a trestných konaní (*Bykov proti Rusku* [VK], 2009, § 80-83 - o odpočúvaní rozhovoru v rámci tajnej policajnej operácie a použití takto získaných dôkazov ako podkladu pre odsúdenie).

7.3.2.4 Dĺžka súdnych konaní týkajúcich sa ochrany údajov

V prípade *Satakunnan Markkinapörssi Oy a Satamedia Oy proti Fínsku* [VK], 2017 (§ 215), ESĽP rozhodol, že celková dĺžka – šesť rokov a šesť mesiacov na dvoch úrovniach jurisdikcie – konania týkajúceho sa zlučiteľnosti s vnútroštátnym právom a právom Európskej únie o hromadnom zverejňovaní osobných údajov o zdaňovaní žiadateľmi - spoločnosťami nespĺňalo požiadavku primeranej lehoty podľa článku 6 ods. 1. Konanie pred Súdnym dvorom Európskej

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

únie týkajúce sa návrhu na začatie prejudiciálneho konania nebolo možné vziať do úvahy pri posudzovaní dĺžky, ktorú možno pripísať vnútroštátnym orgánom (tamže, § 208).

Na rozdiel od toho, v prípade *Surikov proti Ukrajine*, 2017 (§ 104-106), ESĽP označil sťažnosť týkajúcu sa dĺžky konania týkajúceho sa uchovávania citlivých a neaktuálnych informácií o duševnom zdraví zamestnanca a ich využití pri skúmaní jeho žiadosti o povýšenie zo strany zamestnávateľa za zjavne neopodstatnenú. ESĽP zistil, že obdobie kratšie ako šesť rokov na troch úrovniach jurisdikcie nevyvolalo problém, pokiaľ ide o požiadavku primeraného času podľa článku 6 ods. 1 (tamže, § 101).

7.3.2.5 Právo na účinný prostriedok nápravy (článok 13 Dohovoru)

V prípade Klass a ďalší proti Nemecku, 1978 (§ 65-72), zákon „G10“ umožnil úradom otvárať a kontrolovať poštu, čítať telegrafické správy a počúvať a nahrávať telefonické rozhovory, s cieľom brániť krajinu pred „bezprostredným nebezpečenstvom“. ESĽP rozhodol, že súhrn opravných prostriedkov ustanovených v nemeckom práve spĺňal za osobitných okolností tohto prípadu požiadavky článku 13 vo svetle článku 8 týkajúce sa rešpektovania súkromného života a korešpondencie. Aj keď podľa zákona nariadenie a výkon obmedzujúcich opatrení nebolo možné napadnúť na súde, jednotlivci, ktorí sa domnievali, že sú pod dohľadom, mali k dispozícii rôzne iné opravné prostriedky. Podľa rozsudku Spolkového ústavného súdu z roku 1970 bol príslušný orgán povinný informovať dotknutú osobu hneď, ako boli opatrenia dohľadu prerušené, pričom oznámenie bolo možné vykonať bez ohrozenia účelu obmedzenia. Od momentu takéhoto oznámenia boli jednotlivcom k dispozícii rôzne opravné prostriedky pred súdmi. Mohli by: podať určovaciu žalobu s cieľom dosiahnuť, aby správne súdy preskúmali, či sa G10 v ich prípade uplatnila zákonne a či nariadené opatrenia dohľadu boli v súlade so zákonom; podať žalobu o náhradu škody na občianskom súde, ak boli poškodené; alebo podať žalobu na zničenie alebo prípadne vrátenie dokumentov. Nakoniec, ak žiadny z týchto opravných prostriedkov nebol úspešný, mohli sa obrátiť na Spolkový ústavný súd, aby rozhodol, či došlo k porušeniu základného zákona. Pozri v podobnom zmysle aj prípady *Leander proti Švédsku*, 1987 (§ 78-84) ohľadne systému tajných previerok kandidátov na zamestnanie na dôležitých pozíciách z hľadiska národnej bezpečnosti, a *Amann proti*

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Švajčiarsku [VK], 2000 (§ 89-90) ohľadne odpočúvania a nahrávania telefonického hovoru a uchovávania osobných údajov spravodajskými službami.

7.3.3 Vybrané rozhodnutia ESĽP – bližšie vymedzenie prípadov a ich zhrnutia

7.3.3.1 GPS dáta

Florindo de Almeida Vasconcelos Gramaxo proti Portugalsku

Tento prípad sa týkal prepustenia sťažovateľa na základe údajov získaných z geolokačného systému namontovaného v aute, ktoré mu dal zamestnávateľ k dispozícii na účely výkonu práce lekárskeho zástupcu. Žalobca tvrdil, že spracovaním geolokačných údajov získaných zo systému GPS nainštalovaného v jeho služobnom vozidle a použitím týchto údajov ako základu pre jeho prepustenie bolo porušené jeho právo na rešpektovanie jeho súkromného života. Sťažoval sa tiež, že konanie pred vnútroštátnymi súdmi bolo nespravodlivé, keďže rozhodnutia súdov boli založené takmer výlučne na nezákonných dôkazoch získaných prostredníctvom systému GPS nainštalovaného v jeho služobnom vozidle.

ESĽP rozhodol, že nedošlo k porušeniu článku 8 Dohovoru, pričom konštatoval, že vnútroštátne orgány nedodržali svoju pozitívnu povinnosť chrániť právo sťažovateľa na rešpektovanie jeho súkromného života. V úvode uviedol, že žalobca vedel o tom, že spoločnosť nainštalovala do jeho vozidla systém GPS s cieľom monitorovať prejdené vzdialenosti pri výkone jeho profesionálnej činnosti a prípadne pri súkromných cestách. Poznamenal tiež, že odvolací súd tým, že zohľadnil len geolokačné údaje týkajúce sa prejdených vzdialeností, zredukoval rozsah zásahu do súkromného života sťažovateľa na to, čo bolo nevyhnutne potrebné na dosiahnutie sledovaného legitímneho cieľa, ktorým je sledovanie výdavkov spoločnosti. V prípade sťažovateľa mal ESĽP za to, že odvolací súd vykonal podrobnú rovnováhu medzi právom sťažovateľa na rešpektovanie jeho súkromného života a právom jeho zamestnávateľa na zabezpečenie plynulého chodu spoločnosti s prihliadnutím na legitímny sledovaný cieľ spoločnosti, a to právo sledovať jej výdavky. Štát teda v tomto prípade neprekročil svoju mieru voľnej úvahy. ESĽP tiež rozhodol, že nedošlo k porušeniu článku 6 ods. 1 (právo na spravodlivý proces) Dohovoru, keď zistil, že použitie geolokačných údajov

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

týkajúcich sa vzdialeností prejdených sťažovateľom v jeho služobnom vozidle ako dôkazu nenarušil spravodlivosť konania v prejednávanej veci.

7.3.3.2 Monitorovanie používania počítača zamestnancami

Bărbulescu proti Rumunsku (VK)

V tomto prípade išlo o rozhodnutie súkromnej spoločnosti prepustiť zamestnanca – žalobcu – po sledovaní jeho elektronickej komunikácie a prístupe k jej obsahu. Sťažovateľ bol prepustený preto, že počas pracovného času používal internet svojho zamestnávateľa v rozpore s vnútornými predpismi. Zamestnávateľ monitoroval jeho komunikáciu a počas konania pred vnútroštátnym súdom boli predložené záznamy, ktoré obsahovali správy čisto súkromnej povahy. Sťažovateľ sa sťažoval, že rozhodnutie jeho zamestnávateľa bolo založené na porušení jeho súkromia a že vnútroštátne súdy nechránili jeho právo na rešpektovanie jeho súkromného života a korešpondencie.

Veľká komora rozhodla jedenástimi hlasmi proti šiestim, že došlo k porušeniu článku 8 Dohovoru, pričom konštatovala, že rumunské orgány dostatočne nechránili právo sťažovateľa na rešpektovanie jeho súkromného života a korešpondencie. V dôsledku toho nedokázali nájsť spravodlivú rovnováhu medzi dotknutými záujmami. Vnútroštátne súdy najmä neurčili, či bol sťažovateľ vopred upozornený od svojho zamestnávateľa na možnosť monitorovania jeho komunikácie; nezohľadnili ani skutočnosť, že nebol informovaný o povahe alebo rozsahu monitorovania, ani o miere zasahovania do jeho súkromného života a korešpondencie. Okrem toho vnútroštátne súdy neurčili, po prvé, konkrétne dôvody odôvodňujúce zavedenie monitorovacích opatrení; po druhé, či zamestnávateľ mohol použiť opatrenia, ktoré by menej zasahovali do súkromného života a korešpondencie žiadateľa; a po tretie, či nebolo možné získať prístup ku komunikácii bez jeho vedomia.

Libert proti Francúzsku

Tento prípad sa týkal prepustenia zamestnanca SNCF (Francúzska národná železničná spoločnosť) po tom, čo zhabanie jeho pracovného počítača odhalilo uchovávanie pornografických súborov a sfalšovaných certifikátov vyhotovených pre tretie osoby.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Sťažovateľ sa sťažoval najmä na to, že jeho zamestnávateľ otvoril v jeho neprítomnosti osobné súbory uložené na pevnom disku jeho pracovného počítača.

ESĽP rozhodol, že nedošlo k žiadnemu porušeniu článku 8 Dohovoru, pričom konštatoval, že v tomto prípade francúzske orgány neprekročili mieru voľnej úvahy, ktorú mali k dispozícii. ESĽP predovšetkým poznamenal, že nahliadnutie do súborov zamestnávateľom sťažovateľa sledovalo legitímny cieľ ochrany práv zamestnávateľov, ktorí by mohli legitímne chcieť zabezpečiť, aby ich zamestnanci používali počítačové zariadenia, ktoré im dali k dispozícii, v súlade so svojimi zmluvnými záväzkami a platnými predpismi. ESĽP tiež poznamenal, že francúzske právo obsahuje mechanizmus ochrany súkromia, ktorý umožňuje zamestnávateľom otvárať profesionálne spisy, hoci nemohli tajne otvárať spisy označené ako osobné. Posledný typ súborov mohli otvárať iba v prítomnosti zamestnanca. Vnútroštátne súdy rozhodli, že uvedený mechanizmus by nebránil zamestnávateľovi otvoriť sporné spisy, keďže neboli riadne označené ako súkromné. Napokon sa ESĽP domnieval, že vnútroštátne súdy správne posúdili sťažovateľovo tvrdenie o porušení jeho práva na rešpektovanie jeho súkromného života a že rozhodnutia týchto súdov boli založené na relevantných a dostatočných dôvodoch.

7.3.3.3 Video dohľad

Köpke proti Nemecku (rozhodnutie o prípustnosti sťažnosti)

Sťažovateľka, pokladníčka v supermarkete, bola bez upozornenia prepustená z dôvodu krádeže po utajenej videosledovacej operácii, ktorú vykonal jej zamestnávateľ s pomocou súkromnej detektívnej agentúry. Svoju výpoveď neúspešne napadla na pracovnom súde. Rovnako bola zamietnutá aj jej ústavná sťažnosť.

ESĽP zamietol sťažnosť sťažovateľky podľa článku 8 Dohovoru ako neprípustnú (zjavne nepodloženú). Dospel k záveru, že vnútroštátne orgány dosiahli spravodlivú rovnováhu medzi právom zamestnankyne na rešpektovanie jej súkromného života a záujmom jej zamestnávateľa na ochrane jeho vlastníckych práv a verejným záujmom na riadnom výkone spravodlivosti. ESĽP však poznamenal, že dotknutým konkurenčným záujmom by sa v

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

budúcnosti mohla prisúdiť iná váha vzhľadom na rozsah, v akom nové, čoraz sofistikovanejšie technológie umožňovali zásahy do súkromného života.

Antović a Mirković proti Čiernej Hore

Tento prípad sa týkal sťažnosti na narušenie súkromia dvoch profesorov Matematickej fakulty na Univerzite v Čiernej Hore po tom, čo bol v oblastiach, kde vyučovali, nainštalovaný kamerový systém. Uviedli, že nemali žiadnu účinnú kontrolu nad zhromaždenými informáciami a že sledovanie bolo nezákonné. Vnútroštátne súdy však zamietli žiadosť o odškodnenie a zistili, že otázka súkromného života nebola sporná, keďže posluchárne, v ktorých sťažovatelia vyučovali, boli verejné priestory.

ESĽP rozhodol, že došlo k porušeniu článku 8 Dohovoru, keď konštatoval, že kamerové sledovanie nebolo v súlade so zákonom. Najprv odmietol argument vlády, že prípad je neprípustný, pretože nešlo o žiadnu otázku súkromia, keďže sledovaná oblasť bola verejnou, pracovnou oblasťou. V tejto súvislosti ESĽP najmä poznamenal, že už predtým zistil, že súkromný život môže zahŕňať profesionálne činnosti, a usúdil, že to bol aj prípad sťažovateľov. Preto bol uplatniteľný článok 8. Pokiaľ ide o podstatu prípadu, ESĽP potom konštatoval, že kamerové sledovanie predstavovalo zásah do práva sťažovateľov na súkromie a že dôkazy preukázali, že toto sledovanie porušilo ustanovenia vnútroštátneho práva. Vnútroštátne súdy totiž nikdy ani nezvažovali žiadne právne opodstatnenie sledovania, pretože od začiatku rozhodli, že k žiadnemu narušeniu súkromia nedošlo.

López Ribalda a ďalší proti Španielsku (VK)

Tento prípad sa týkal utajeného videosledovania zamestnancov, ktoré viedlo k ich prepusteniu. Sťažovatelia sa sťažovali na utajené videosledovanie a na to, ako španielske súdy použili získané údaje na zistenie, že ich prepustenie bolo spravodlivé. Sťažovatelia, ktorí podpísali dohody o urovnaní, sa tiež sťažovali, že dohody boli uzavreté pod nátlakom kvôli video materiálu a nemali byť akceptované ako dôkaz, že ich prepustenie bolo spravodlivé.

Veľká komora ESĽP rozhodla, že v súvislosti s piatimi sťažovateľmi nedošlo k porušeniu článku 8 Dohovoru. Konštatovala najmä, že španielske súdy starostlivo vyvážili práva sťažovateľov – zamestnancov supermarketu podozrivých z krádeže – a práva zamestnávateľa a dôkladne

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

preskúmali opodstatnenosť video sledovania. Kľúčovým argumentom sťažovateľov bolo, že napriek takejto zákonnej požiadavke nedostali predchádzajúce oznámenie o sledovaní, ale ESĽP zistil, že takéto opatrenie má jasné opodstatnenie z dôvodu dôvodného podozrenia zo závažného pochybenia a stratám, berúc do úvahy rozsah a dôsledky opatrenia videosledovania. V tomto prípade teda vnútroštátne súdy neprekročili svoju právomoc voľnej úvahy („*margin of appreciation*"), keď považovali monitorovanie za primerané a legitímne. ESĽP tiež rozhodol, že nedošlo k porušeniu článku 6 ods. 1 (právo na spravodlivý proces) Dohovoru, pričom najmä konštatoval, že použitie video materiálu ako dôkazu nenarušilo spravodlivosť súdneho konania.

7.3.3.4 Trestnoprávny kontext

M.M. proti Spojenému kráľovstvu

V roku 2000 sťažovateľku zatkla polícia po tom, čo na jeden deň zmizla so svojím malým vnukom v snahe zabrániť jeho odchodu do Austrálie po rozpade manželstva jej syna. Úrady sa rozhodli, že ju nebudú stíhať a namiesto toho jej udelili pokarhanie za únos dieťaťa. Toto pokarhanie malo pôvodne zostať v zázname päť rokov, ale v dôsledku zmeny politiky v prípadoch, keď poškodenou stranou bolo dieťa, sa toto obdobie neskôr predĺžilo na doživotie. Sťažovateľka sa sťažovala na neobmedzené uchovávanie a zverejňovanie údajov o jej pokarhaní a na vplyv toho na jej vyhliadky na zamestnanie.

ESĽP rozhodol, že došlo k porušeniu článku 8 Dohovoru. V dôsledku kumulatívneho účinku zistených nedostatkov skutočne nebolo preukázané, že v systéme uchovávania a zverejňovania údajov z registra trestov existujú dostatočné záruky, ktoré by zabezpečili, že údaje týkajúce sa súkromného života sťažovateľky nebudú zverejnené v rozpore s jej právom na rešpektovanie súkromného života. Uchovávanie a sprístupnenie údajov o pokarhaní sťažovateľky preto nemožno považovať za súladné so zákonom podľa článku 8. ESĽP predovšetkým poznamenal, že hoci údaje obsiahnuté v registri trestov boli v istom zmysle verejné, informácie a ich systematické uchovávanie v centrálnej evidencii znamenali, že boli k dispozícii na zverejnenie dlho po udalosti, keď na ne všetci okrem dotknutej osoby pravdepodobne zabudli, najmä ak, ako v prípade sťažovateľky, k pokarhaniu došlo neverejne.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Ako teda samotné presvedčenie či opatrnosť ustupovali do minulosti, stali sa súčasťou súkromného života človeka, ktorý bolo potrebné rešpektovať.

7.3.3.5 Uchovávanie v tajných registroch

Leander proti Švédsku

Tento prípad sa týkal použitia spisu tajnej polície pri nábore stolára. Sťažovateľ, ktorý pracoval ako dočasná náhrada v Námornom múzeu v Karlskrone, vedľa vojenskej bezpečnostnej zóny, sa dlho predtým sťažoval na uchovávanie údajov súvisiacich s jeho odborovými aktivitami a tvrdil, že to viedlo k jeho vylúčeniu z predmetného zamestnania. Tvrdil, že nič v jeho osobnom alebo politickom pozadí nemožno považovať za také, aby bolo potrebné zaregistrovať ho v registri bezpečnostného oddelenia a klasifikovať ho ako „bezpečnostné riziko“.

ESĽP rozhodol, že nedošlo k porušeniu článku 8 Dohovoru. Poukazuje najmä na to, že tak uchovávanie v tajnom registri, ako aj zverejňovanie informácií o súkromnom živote jednotlivca patrí do pôsobnosti článku 8 Dohovoru. ESĽP tiež pripomenul, že v demokratickej spoločnosti existencia spravodajských služieb a uchovávanie údajov je zákonné a prevažuje nad záujmami občanov za predpokladu, že sleduje legitímne ciele, konkrétne predchádzanie nepokojom alebo zločinu alebo z dôvodu ochrany národnej bezpečnosti. V tomto prípade ESĽP zistil, že záruky obsiahnuté vo švédskom systéme kontroly zamestnancov spĺňajú požiadavky článku 8 Dohovoru a že švédska vláda bola oprávnená domnievať sa, že záujmy národnej bezpečnosti prevažujú nad individuálnymi záujmami sťažovateľa.

7.3.3.6 Zverejnenie osobných údajov

Radu proti Moldavskej republike

Sťažovateľka, lektorka Policajnej akadémie, sa sťažovala na to, že štátna nemocnica zverejnila zdravotné informácie o nej jej zamestnávateľovi. Informácia sa šírila na pracovisku sťažovateľky a krátko nato v dôsledku stresu potratila. Neúspešne podala žalobu na nemocnicu Policajnú akadémiu.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ESĽP rozhodol, že došlo k porušeniu článku 8 Dohovoru, keď konštatoval, že sťažovateľkou namietaný zásah do výkonu práva na rešpektovanie súkromného života nebol „v súlade so zákonom“ v zmysle čl. 8.

Sõro proti Estónsku

Tento prípad sa týkal sťažnosti sťažovateľa na skutočnosť, že informácie o jeho zamestnaní počas sovietskej éry ako vodiča pre Výbor pre štátnu bezpečnosť ZSSR (KGB) boli uverejnené v Estónskom štátnom vestníku v roku 2004.

ESĽP rozhodol, že došlo k porušeniu článku 8 Dohovoru, pričom sa zistilo, že v prípade sťažovateľa bolo toto opatrenie neprimerané k sledovaným cieľom. ESĽP predovšetkým poznamenal, že podľa príslušných vnútroštátnych právnych predpisov sa zverejňovali informácie o všetkých zamestnancoch bývalých bezpečnostných služieb – vrátane vodičov, ako v prípade sťažovateľa – bez ohľadu na konkrétnu funkciu, ktorú vykonávali. Okrem toho, zatiaľ čo zákon o zverejnení nadobudol účinnosť tri a pol roka po vyhlásení nezávislosti Estónska, zverejňovanie informácií o bývalých zamestnancoch bezpečnostných služieb sa natiahlo na niekoľko rokov. V prípade sťažovateľa boli predmetné informácie zverejnené až v roku 2004, takmer 13 rokov po vyhlásení nezávislosti Estónska, a v čase zverejnenia oznámenia neexistovalo žiadne posúdenie možnej hrozby, ktorú sťažovateľ predstavoval. Napokon, hoci samotný zákon o zverejňovaní nestanovil žiadne obmedzenia na zamestnanie sťažovateľa, podľa jeho vyjadrení bol zo strany kolegov zosmiešňovaný a bol nútený opustiť prácu. ESĽP sa domnieval, že aj keď zákon takýto výsledok nepožadoval, svedčí to o tom, aký závažný bol zásah do sťažovateľovho práva na rešpektovanie jeho súkromného života.

7.4 ROZHODOVACIA ČINNOSŤ SÚDNEHO DVORA EÚ

7.4.1 Získavanie údajov o pracovnom príjme jednotlivca

V rámci právnych predpisov EÚ je právo na prístup k dokumentom zaručené nariadením č. 1049/2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (nariadenie o prístupe k dokumentom). Toto právo bolo rozšírené článkom 42 Charty a článkom 15 ods. 3 Zmluvy o fungovaní Európskej únie na prístup „k dokumentom inštitúcií, orgánov, úradov a agentúr Únie bez ohľadu na ich nosič“. Toto právo by sa mohlo dostať do

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

konfliktu s právom na ochranu údajov v prípade, ak by sa sprístupnením dokumentov zverejnili osobné údaje iných osôb. V článku 86 všeobecného nariadenia o ochrane údajov sa jasne ustanovuje, že osobné údaje v úradných dokumentoch, ktoré má v držbe orgán verejnej moci alebo verejnoprávny subjekt, môže daný orgán alebo subjekt poskytnúť v súlade s právom Únie alebo právom členského štátu, s cieľom zosúladiť prístup verejnosti k úradným dokumentom s právom na ochranu osobných údajov podľa tohto nariadenia. Preto je potrebné vyvážiť žiadosti o prístup k dokumentom alebo informáciám uchovávaným verejnými orgánmi s právom na ochranu údajov osôb, ktorých údaje sú obsiahnuté v požadovaných dokumentoch. Príklad: Vo veci *Rechnungshof/Österreichischer Rundfunk a i.*[245] Súdny dvor Európskej únie (ďalej aj ako „SDEÚ“) preskúmal zlučiteľnosť niektorých rakúskych právnych predpisov s právnymi predpismi Európskej únie (ďalej aj ako „EÚ“ alebo „Únia“) o ochrane údajov. Právnymi predpismi sa štátnemu orgánu ukladala povinnosť zhromažďovať a oznámiť údaje o príjmoch na účely zverejnenia mien a príjmov zamestnancov rôznych verejných subjektov vo výročnej správe, ktorá sa sprístupňuje širokej verejnosti. Niektoré osoby odmietli poskytnúť svoje údaje z dôvodu ochrany údajov. SDEÚ vo svojom stanovisku vychádzal z toho, že ochrana základných práv je všeobecnou zásadou v rámci práva EÚ, ako aj z článku 8 Dohovoru, pričom pripomenul, že Charta základných práv EÚ v tom čase nebola záväzná. Skonštatoval, že získavanie údajov o pracovnom príjme jednotlivca, a najmä ich poskytnutie tretím osobám, patrí do rozsahu pôsobnosti práva na rešpektovanie súkromného života a predstavuje porušenie tohto práva. Tento zásah by mohol byť odôvodnený, ak by bol v súlade s právnymi predpismi, sledoval legitímny cieľ a bol v demokratickej spoločnosti nevyhnutný na dosiahnutie tohto cieľa. SDEÚ uviedol, že rakúska právna úprava sledovala legitímny cieľ, keďže jej cieľom bolo udržať platy verejných zamestnancov v rozumných medziach, pričom ide o dôvod, ktorý súvisí aj s hospodárskou prosperitou krajiny. Záujem Rakúska na zabezpečení čo najlepšieho využitia verejných prostriedkov sa však musel vyvážiť so závažnosťou zásahu do práva dotknutých osôb na rešpektovanie ich súkromného života. Hoci určiť, či zverejnenie údajov o príjme fyzických osôb bolo nevyhnutné a primerané cieľu, ktorý sa príslušnými právnymi predpismi sleduje, prináleží vnútroštátnemu súdu, SDEÚ tento

[245] Spojené veci C-465/00, C-138/01 a C-139/01, Rechnungshof/Österreichischer Rundfunk a i. a Christa Neukomm a Joseph Lauermann/Österreichischer Rundfunk, 20. mája 2003.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

súd vyzval, aby preskúmal, či tento cieľ nebolo možné dosiahnuť rovnako účinne aj menej rušivým spôsobom. Príkladom by bolo zasielanie osobných údajov len kontrolným verejným orgánom, a nie širokej verejnosti.[246]

7.4.2 Záznamy o pracovnom čase, zásady týkajúce sa kvality údajov a zákonnosti spracúvania údajov

Podľa všeobecného nariadenia o ochrane údajov by mal mať zamestnanec možnosť jasne odlíšiť údaje, pri ktorých dobrovoľne súhlasí s ich spracúvaním a uchovávaním, a účely, na ktoré sú jeho údaje uchovávané. Zamestnanci by pred udelením súhlasu mali byť informovaní aj o svojich právach a o dĺžke uchovávania údajov. Ak dôjde k porušeniu ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, zamestnávateľ musí toto porušenie oznámiť zamestnancovi. Podľa článku 88 tohto nariadenia sa členským štátom umožňuje stanoviť konkrétnejšie pravidlá na zabezpečenie ochrany práv a slobôd zamestnancov v súvislosti s ich osobnými údajmi v kontexte zamestnania. Príklad: Vo veci *Worten*[247] údaje zahŕňali záznam o pracovnom čase, ktorý obsahoval denný pracovný čas a doby odpočinku, čo predstavuje osobné údaje. Podľa vnútroštátnych právnych predpisov sa môže vyžadovať, aby zamestnávateľ poskytol záznamy o pracovnom čase vnútroštátnym orgánom príslušným v oblasti dohľadu nad pracovnými podmienkami. Išlo by o umožnenie okamžitého prístupu k príslušným osobným údajom. Prístup k osobným údajom je však potrebný na to, aby mohol vnútroštátny orgán vykonávať dohľad nad právnou úpravou pracovných podmienok.[248]

7.5 HLBŠIA ANALÝZA VYBRANÝCH ROZHODNUTÍ ESĽP

7.5.1 Antović a Mirković vs. Čierna Hora - skutkové okolnosti prípadu

Vzhľadom na to, že právna úprava monitoringu nie je podrobne spracovaná a nereflektuje na momentálny technologický vývoj, pri jej realizácii v praxi vznikajú sporné otázky a

[246] Agentúra Európskej únie pre základné práva a Rada Európy. Príručka o európskych právnych predpisoch v oblasti ochrany údajov. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021, s. 65 – 67.
[247] C-342/12, Worten – Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT), 30. mája 2013.
[248] Agentúra Európskej únie pre základné práva a Rada Európy. Príručka o európskych právnych predpisoch v oblasti ochrany údajov. Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2021, s. 343.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

problematické situácie, na ktoré zákon nepozná odpoveď. Jednou z takýchto otázok je aj použitie kamerového systému na sledovanie zamestnancov, o ktorom Zákonník práce mlčí. Ako už bolo spomínané v úvode tejto kapitoly, v takýchto prípadoch je možné hľadať odpovede v rozhodnutia súdov, ktoré pomáhajú odstrániť pochybnosti pri aplikácii právnej úpravy na konkrétne situácie. Medzi takéto rozhodnutia patrí aj rozhodnutie Európskeho súdu pre ľudské práva (ďalej len „ESĽP“) vo veci Antović a Mirković vs. Čierna Hora, v ktorom ESĽP riešil otázku práva na súkromie zamestnancov – univerzitných učiteľov, ktorí boli počas svojich prednášok monitorovaný kamerovým systémom.

Pani Antović a pán Mirković, vyučujúci na Univerzite v Čiernej Hore, sa najskôr domáhali svojho práva súkromie na Úrade na ochranu osobných údajov v Čiernej Hore, keď v roku 2011 podali sťažnosť pre nezákonné monitorovanie a získavanie osobných údajov bez ich súhlasu. Dôvodom podania tejto sťažnosti bolo zavedenie monitorovacieho systému v prednáškových miestnostiach, ktorému predchádzalo informovanie dekanom fakulty v podobe rozhodnutia o zavedení monitoringu. Cieľ tohto opatrenia malo byť zaistenie bezpečnosti majetku a osôb a sledovanie výučby. Prístup k záznamom mal mať výlučne dekan fakulty a údaje mali byť uchovávané po dobu jedného roka. Sťažovatelia sa odvolávali na zákon o ochrane osobných údajov a argumentovali predovšetkým tým, že prednáškové miestnosti sa po skončení prednášky zamykajú a nachádza sa tam len bežné vybavenie. Ďalej tvrdili, že neexistuje žiadny dôvod sa obávať o bezpečnosť osôb a poukazovali na skutočnosť, že existujú aj iné spôsoby na ochranu bezpečnosti. Žiadali o odstránenie kamier a vymazanie kamerových záznamov.

Inšpektori z Úradu na ochranu osobných údajov v Čiernej Hore vo svoje správe však skonštatovali, že monitorovací systém na univerzite je v súlade so zákonom na ochranu osobných údajov. Dôvodili tým, že sa v minulosti na univerzite vyskytovali prípady poškodzovania majetku, študenti nosili na univerzitu zvieratá, alkohol a cigarety a že sa na pôde univerzity vyskytovali ľudia, ktorí neboli študentmi univerzity. V správe takisto uviedli, že kamerový záznam je vykonávaný z diaľky bez jasného rozlíšenia a črty ľudí sa nedajú ľahko rozpoznať. Takisto nebolo možné si obraz priblížiť a nevykonával sa ani hlasový záznam. Inšpektori ďalej zistili, že napriek tomu, že rozhodnutie dekana ustanovovalo dobu uchovania

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

záznamov na jeden rok, kapacita na serveri dovoľovala uchovávať údaje len po dobu 30 dní, následne načo boli údaje automaticky vymazané a nahradené novými záznamami.

V nadväznosti na správu Úradu na ochranu osobných údajov sťažovatelia namietali, že si nie sú vedomí žiadnych prípadov spomínaných v správe, a aj v prípade, že by sa takéto prípady na univerzite vyskytli, nie je jasné akým spôsobom by kamery zaistili bezpečnosť osôb a majetku. Skonštatovali, že kamery pri vstupe do budovy univerzity by možno mohli predstavovať primeranú formu zaistenia takejto bezpečnosti. Okrem toho tvrdili, že zamestnanci neboli písomne oboznámení o systéme monitorovania pred jeho zavedením. Rozhodnutie dekana bolo vydané 24.2.2011, no monitorovanie sa začalo niekoľko týždňov predtým, približne od začiatku februára 2011.

28. apríla 2011 po tom, ako sťažovatelia doručili svoje námietky ku správe, Rada Úradu na ochranu osobných údajov vydala rozhodnutie ukladajúce Fakulte matematiky na Univerzite v Čiernej Hore povinnosť, aby odstránila kamery z prednáškových miestností v lehote 15 dní z dôvodu, že kamerový systém nie je v súlade so zákonom na ochranu osobných údajov. Konkrétne pre nesplnenie zákonných dôvodov nevyhnutných na zavedenie monitorovacieho systému, medzi ktoré Rada zaradila aj existenciu preukázateľného dôkazu o tom, že bezpečnosť osôb a majetku je ohrozená. Rada skonštatovala, že takéto nebezpečenstvo v prednáškových miestnostiach priamo nehrozilo a samotné sledovanie prednášok nie legitímnym dôvodom pre monitorovanie. Žiadna zo strán nepodala voči tomuto rozhodnutiu odvolanie.

V januári 2012 bolo rozhodnutie Rady zo dňa 28. apríla 2011 doručené Fakulte matematiky na Univerzite v Čiernej Hore, následne načo boli kamery odstránené.

Vzápätí nato však sťažovatelia podali na súd žalobu na náhradu škody proti univerzite, Úradu na ochranu osobných údajov a zároveň proti štátu Čierna Hora z dôvodu porušenia ich práva na súkromný život, najmä za nedovolené zbieranie a spracúvanie osobných údajov. Odvolávali sa na zákon o ochrane osobných údajov, článok 8 Dohovoru základných práv a slobôd a príslušnej judikatúry. Súdy však došli k záveru, že natáčanie prednáškových ako verejných miest nemohlo porušiť právo sťažovateľov na ochranu ich súkromného života, keďže sa

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

jednalo o inštitúciu vykonávajúci činnosti vo verejnom záujme (medzi ktoré patrí aj výučba). Prednáškové miestnosti sú podľa názoru súdov pracovným priestorom, rovnaký akým je napríklad súdna sieň nebo parlament, v ktorom neboli vyučujúci nikdy sami, a preto sa nemohli dovolávať zásahu do svojho súkromného života.

Po vyčerpaní všetkých vnútroštátnych prostriedkov súdnej ochrany sa pani Antović a pán Mirković obrátili na ESĽP, kde namietali, že Čierna Hora ako signatár Dohovoru o ochrane ľudských práv a slobôd, porušila čl. 8, ktorý zaručuje právo každého na rešpektovanie rodinného, súkromného života, obydlia a korešpondencie.

7.5.1.1 Analýza rozhodnutia ESĽP vo veci Antović a Mirković vs. Čierna Hora

Sťažovatelia v súlade s Článkom 8 Európskeho dohovoru o ochrane ľudských práv a slobôd (ďalej len „**Dohovor**“) namietali nelegálnosť inštalácie a používania monitorovacieho zariadenia (videozáznam) v prednáškovej miestnosti univerzity, skutočnosť ktorá predstavuje zásah do ich práva na súkromný život. Relevantné znenie Článku 8 Dohovoru, na ktorý sťažovatelia odkazovali znie:

„1. Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a korešpondencie.

2. Štátny orgán nemôže do výkonu tohto práva zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných.“[249]

V súvislosti so skúmaním prípustnosti aplikácie Článku 8 Dohovoru na prípad Antović a Mirković vs. Čierna hora vláda Čiernej hory namietala aplikáciu Článku 8 argumentujúc, že nie všetky profesijné a obchodné aktivity môžu byť zahrnuté do oblasti súkromného života. Univerzita, na pôde ktorej došlo k inštalácii monitorovacieho zariadenia je verejná inštitúcia a výučba je aktivitou vo verejnom záujme. Monitorované priestory predstavujú pracovisko

[249] Článok 8 Dohovoru o ochrane ľudských práv a základných slobôd

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

sťažovateľov, ktoré je mimo rozsahu ich osobnej autonómie, na rozdiel od kancelárií vyučujúcich, kde im istá miera osobnej autonómie bola poskytovaná.

Pri posudzovaní prípustnosti aplikácie Článku 8 Dohovoru vychádzal Európsky súd pre ľudské práva v Štrasburgu (ďalej len „**Súd**“) z princípov stanovených rozhodnutiami Súdu v prípadoch ako *Niemetz v. Nemecko* (16.12.1992, §§ 29 – 31, Séria 1 č. 251 – B); *Peck v. Spojené kráľovstvo Veľkej Británie a Severného Írska* (č. 44647/98, §§ 57-58, 2003 – I); *Halford v. Spojené kráľovstvo Veľkej Británie a Severného Írska* (25.06.1997, §§ 44-46), *Fernández Martinéz v. Španielsko* (č. 56030/07, §§ 109-110); a *Barbulescu v. Rumunsko* (č. 61496/08, §§ 70-73).

Podľa názoru Súdu nie je správne limitovať obsah pojmu „súkromný život“ príliš reštriktívne, t.j. len na „vnútorný okruh“ človeka s absolútnym vylúčením vonkajšieho sveta (*Niemietz, §29*)[250]. Článok 8 Dohovoru zahŕňa aj právo na „spoločenský život“, ktorý umožňuje jednotlivcom rozvíjať sociálnu identitu. V takomto vnímaní právo na súkromie zahŕňa aj oprávnenie oslovovať ostatných s cieľom nadviazať a rozvíjať s nimi sociálne väzby (*Barbulescu, § 70*)[251]. Právo na súkromný život tak môže zahŕňať aj profesijné aktivity a aktivity realizované na verejnosti, nakoľko väčšina ľudí nadväzuje nové sociálne väzby najčastejšie v časti spadajúcej do ich pracovného života. Z uvedeného dôvodu existuje istá zóna interakcie s ostatnými, ktorá spadá do obsahu pojmu „súkromný život“, ktorého súčasťou je aj profesijná oblasť (*Fernandez Martines, § 110*)[252].

Po aplikácii horeuvedených princípov na rozoberaný prípad Antović a Mirković vs. Čierna hora Súd poznamenal, že prednáškové miestnosti je potrebné považovať za pracovisko učiteľov (sťažovateľov). Ide tak o priestor, v ktorom vyučujúci nielen učia študentov, ale realizujú aj sociálne interakcie, rozvíjajú vzájomné vzťahy a budujú svoju sociálnu identitu. Už bolo rozhodnuté, že skryté monitorovanie zamestnanca na jeho pracovisku musí byť ako také považované za značný zásah do jeho súkromného života. Zahŕňa zaznamenanú a reprodukovateľnú dokumentáciu správania sa osoby na pracovisku, ktorej sa zamestnanec,

[250] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Niemetz v. Nemecko z 16.12.1992
[251] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Barbulescu v. Rumunsko, žiadosť č. 61496/08
[252] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Fernández Martínez v. Španielsko, žiadosť č. 56030/07

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

povinný podľa pracovnej zmluvy vykonávať prácu na tomto mieste, nemôže vyhnúť (*Köpke v. Nemecko*)[253]. Aj keď sú predpisy zamestnávateľa týkajúce sa súkromného života zamestnancov na pracovisku reštriktívne, nemôžu ho znížiť na nulu. Rešpektovanie súkromného života naďalej existuje, aj keď by to mohlo byť v prípade potreby obmedzené (*Barbulescu, § 80*)[254].

Vzhľadom na vyššie uvedené Súd rozhodol, že monitorovanie zamestnancov sa vzťahuje aj na oblasť ich súkromného života a preto je Článok 8 Dohovoru na prípad Antović a Mirković vs. Čierna hora aplikovateľný.

V súvislosti so samotným meritom prípadu sťažovatelia (vysokoškolskí profesori Antović a Mirković) napadli video monitoring prednáškových miestností ako nezákonný, nesledujúci legitímny cieľ a nepotrebný v demokratickej spoločnosti, t.j. nespĺňajúci základné princípy zásahov do ľudských práv a slobôd. Argumentovali, že dekan školy zbieral a spracovával dáta získané bez akéhokoľvek obmedzenia a dotknuté osoby nedisponovali efektívnym nástrojom kontroly v súvislosti so spracúvanými informáciami.

Vláda Čiernej hory na svoju obranu uvádza, že dohľad nad činnosťami, ktoré sa uskutočnili na verejnosti alebo s fotografickým zariadením nie je považovaný za zásah do súkromného života osôb pokým nedošlo k zverejneniu – tak ako v tomto prípade. Taktiež tvrdí, že zavedenie monitorovacieho systému bolo v súlade s právom, sledovalo legitímny cieľ a bolo nevyhnutné pre demokratickú spoločnosť. Ciel použitia monitorovacieho systému nebolo možné dosiahnuť menej invazívnym spôsobom a predstavuje nástroj prevencie a riešenia incidentov súvisiacich s bezpečnosťou, akými sú krádeže a vlámania, počas ktorých bol ukradnutý majetok tak študentov ako aj profesorov. Taktiež má slúžiť ako prevencia vnášania zbraní a nepovolených zvierat do priestorov prednáškovej miestnosti ako aj incidentov, počas ktorých došlo k fyzickému napadnutiu profesorov. Inštalácia obdobného zariadenia mala byť dokonca odporúčaná zo strany polície.

[253] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Köpke v. Nemecko, žiadosť č. 420/07
[254] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Barbulescu v. Rumunsko, žiadosť č. 61496/08

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Ďalej vláda tvrdila, že všetci zúčastnení, vrátane sťažovateľov, boli o tomto zavádzanom opatrení riadne vopred informovaní, a že zozbierané údaje neboli nijakým spôsobom zneužité a mal k nim prístup výlučne dekan školy. Údaje tiež mali byť použiteľné len v obmedzenom čase, keďže boli automaticky vymazané po tridsiatich dňoch.

Európsky súd pre ľudské práva už v obdobnej veci rozhodol, že monitorovanie zamestnancov (či už skryté alebo nie) je považované za zásah do práva zamestnancov na súkromie. Prípadný zásah do práva na súkromie musí byť v súlade s Článkom 8 ods. 2 Dohovoru, t. j. musí sledovať niektorý z legitímnych cieľov článkom stanovených, musí byť nevyhnutný v demokratickej spoločnosti a v súlade so zákonom (*Vukota-Nojič v. Švajčiarsko, § 60*)[255].

Súd má za to, že vnútroštátny súd Čiernej hory riadne nepreskúmal splnenie zákonnosti zavedenia monitorovacieho systému, nakoľko v danom prípade nepredpokladal existenciu zásahu do práva na súkromie, a tým neskúmal splnenie zákonných podmienok na zásah. Takéto posúdenie však vykonal vnútroštátny Úrad na ochranu osobných údajov, ktorý zistil porušenie ustanovení 10, 35 a 36 Zákona o ochrane osobných údajov.

Súd v tejto súvislosti poznamenáva, že ustanovenie 35 stanovuje, že verejné inštitúcie – medzi ktoré patria podľa názoru vlády aj univerzity - môžu vykonávať dohľad prostredníctvom kamerových systémov v oblastiach prístupu do priestorov. V prejednávanej veci sa však kamerový dohľad vykonáva v celej prednáškovej miestnosti.

Okrem toho ustanovenie 36 Zákona o ochrane osobných údajov stanovuje, že monitorovacie zariadenia môžu byť inštalované aj v úradných alebo obchodných priestoroch, len vtedy, ak cieľ ako bezpečnosť osôb alebo majetku alebo ochrana dôverných informácií, nie je možné dosiahnuť menej invazívnym spôsobom. Súd poznamenáva, že v tomto prípade bol zavedený kamerový systém za účelom zabezpečenia bezpečnosti majetku a osôb, vrátane študentov, a dohľadu nad vyučovaním. Treba poznamenať, že jeden z týchto cieľov, najmä dohľad nad vyučovaním, zákon vôbec nestanovuje ako oprávnený dôvod na zavedenie kamerového systému. Úrad pre ochranu osobných údajov okrem toho výslovne konštatoval, že neexistujú dôkazy o tom, že by bol majetok alebo ľudia v škole v reálnom v ohrození a vnútroštátne súdy

[255] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Vukota-Nojič v. Švajčiarsko, žiadosť č. 61838/10

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

sa touto otázkou vôbec nezaoberali. Vláda na druhej strane opak nedokázala a pred zavedením monitorovacieho systému univerzity nezvážila efektivitu iného, menej invazívneho spôsobu zabezpečenia ochrany majetku a osôb.

Vzhľadom na vyššie uvedené Súd rozhodol, že v prípade Antović a Mirković vs. Čierna hora došlo porušenia Článku 8 Dohovoru, nakoľko neboli splnené základné predpoklady legálneho obmedzenia práva na súkromie, a to:

1. Jedným z dôvodov zavedenia monitorovacieho systému bol dohľad nad vyučovaním. Tento dôvod nevychádza zo žiadneho zákonného oprávnenia, t.j. legitimity cieľa nie je naplnená.
2. Pred zavedením monitorovacieho systému nedošlo ani k teoretickému zváženiu menej invazívneho spôsobu zabezpečenia bezpečnosti osôb a majetku, t.j. nedošlo k naplneniu podmienky nevyhnutného rozsahu.
3. Samotná hrozba pre bezpečnosť osôb a majetku nebola zo strany vlády preukázaná reálnymi prípadmi, ktorými k ohrozeniu alebo narušeniu bezpečnosti došlo, t.j. nie je možné preukázať reálnu hrozbu, ktorá odôvodňuje invazívny zásah do práva na súkromie, akým je monitorovanie prednáškových miestností.

Prílohou Rozsudku Európskeho súdu pre ľudské práva v Štrasburgu bolo aj spoločné stanovisko sudcov Vučinić a Lemmens, ktorí plne súhlasili s výrokom o porušení Článku 8 Dohovoru zavedením monitorovacieho systému v prednáškovej miestnosti, avšak preferovali by mierne odlišné zdôvodnenie.

Podľa názoru sudcov Vučinić a Lemmens dôležitým aspektom práva na súkromný život je „právo žiť súkromne, bez nechcenej pozornosti“ (*Smirnova v. Rusko, § 95*).[256]

V prípade Antović a Mirković vs. Čierna hora nehovoríme o umiestnení bezpečnostných kamier napríklad pri vchodoch a východoch univerzitnej budovy. Ide o monitorovanie prednáškových priestorov. Pri zabezpečení bezpečnosti osôb a majetku ako jedného z cieľov

[256] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Smirnova v. Rusko, žiadosť č. 46133/99 a 48183/99

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

opatrenia Úrad na ochranu osobných údajov nepovažoval odôvodnenie zamýšľaného cieľa monitorovania za dôveryhodné – práve naopak, zdôvodnenie monitorovania vzdelávacej činnosti a prístup k nahrávkam len zo strany dekana vedie k podozreniu, že hlavným cieľom zavedenia monitorovacieho systému bolo kontrolovať výučbu profesorov.

Prednáškové miestnosti nie sú len verejným, ale aj súkromným miestom. Sú to priestory, kde sa učitelia stretávajú so svojimi študentami a vznikajú medzi nimi interakcie. Tieto interakcie nie sú výlučne sociálnej povahy. Ide o špecifický vzťah. Učitelia učia študentov, ktorí sú zaradení do ich triedy. Vzťah medzi učiteľom a študentom sa vyvíja počas celej výučby, celého semestra. Javí sa ako prirodzené, že učiteľ očakáva istú mieru súkromia, a to čo sa deje v triede majú právo sledovať tí, ktorí sú súčasťou triedy. Nie je žiadaná nechcená pozornosť od osôb, ktoré nemajú s triedou nič spoločné. Práve v akademickom prostredí, kde akademická výučba má niesť známky akademickej slobody, sa očakávanie súkromia môže považovať za „dôvodné“.

Súčasťou Rozsudku však bolo aj nesúhlasné stanovisko sudcov Stano, Bianku a Kjølbro, ktorí zastávajú názor, že na prípad Antović a Mirković vs. Čierna hora nie je možné aplikovať Článok 8 Dohovoru.

Súd mnohokrát rozhodol v prípadoch súvisiacich s monitorovaním pracovísk, že monitorovanie zamestnancov zo strany zamestnávateľa samo o sebe automaticky neznamená zásah do súkromného života zamestnancov a aplikáciu Článku 8 Dohovoru.

Sudcovia Stano, Bianku a Kjølbro vo svojom vyjadrení súhlasili s názorom vlády Čiernej hory, že monitorovanie prednáškovej činnosti nezasahuje do práva profesorov na súkromie. Monitorovanie kamerovým systémom prebiehalo v prednáškových miestnostiach, o tejto skutočnosti boli profesori vopred informovaní, taktiež nedochádzalo k vyhotovovaniu zvukového záznamu, t.j. diskusie vyučujúcich so žiakmi nahrávané neboli, video záznamy boli k dispozícii len dekanovi a boli automaticky vymazané po uplynutí 30 dní.

Názor sudcov sa líši s názorom väčšiny v myšlienke, že samotné monitorovanie priestoru kamerovým systémom neznamená automaticky zásah do práva na súkromie monitorovaných osôb. Sťažovatelia sú totiž univerzitní učitelia, ktorí v priestoroch prednáškovej miestnosti

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

vykonávajú výlučne odbornú, profesijnú aktivitu. Boli vopred informovaný o monitorovaní prednáškovej miestnosti, preto akékoľvek očakávanie súkromia, ak vôbec nejaké bolo, muselo byť limitované. Vyučujúci môžu legitímne očakávať zachovanie súkromia napr. vo svojich kanceláriách.

Sťažovatelia boli vopred informovaní o kamerovom systéme, nedochádzalo k prenosu zvuku, t.j. diskusie so žiakmi neboli nahrávané a jednalo sa o priestory, v ktorým má prebiehať výlučne prednášková činnosť, t.j. priestory, v ktorým učitelia v plnej miere vykonávajú svoje zamestnanie.

7.5.1.2 Záverečné zhrnutie

Rozhodnutie Európskeho súdu pre ľudské práva v Štrasburgu vo veci Antović a Mirković vs. Čierna hora je argumentačne zamerané predovšetkým na otázku obsahovej náplne pojmu „súkromný život". Hranica medzi súkromným životom a pracovnou oblasťou je výslovne tenká, a mnohokrát závisí od uhla pohľadu rozhodujúceho orgánu. Jedná sa však o rozhodujúce posúdenie z hľadiska možnej aplikácie Článku 8 Dohovoru o ochrane ľudských práv a základných slobôd. Podľa Ústavného súdu SR Dohovor zakladá legitimitu zásahu do práva na súkromie len v prípadoch, že to vyžaduje záujem národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných. Rovnako však podľa Ústavného súdu musí byť dodržaná aj zásada proporcionality uvedeného zásahu, ktorý je podľa neho prípustný, len ak je to v demokratickej spoločnosti nevyhnutné v záujme dosiahnutia legitímneho cieľa.[257] Súhlasíme s názorom prof. Barancovej, že takýto zásah do súkromia je možný, len keď je to nevyhnutné, keď legitímny cieľ nie je možné dosiahnuť miernejšími prostriedkami pri doržaní zásad a princípov demokratickej spoločnosti.[258]

Na strane druhej sme však toho názoru, že nevyhnutným kritériom pre posúdenie oblasti zásahu prostredníctvom monitorovacích zariadení do súkromia je legitímnosť očakávania súkromia zo strany dotknutej osoby, t. j. či je v danej pozícii a na danom mieste oprávnená

[257] Nález Ústavného súdu Slovenskej republiky č. I. ÚS 117/2007 z dňa 4. 2. 2009
[258] Porov. BARANCOVÁ, H.: Nové technológie v pracovnoprávnych vzťahoch. Praha: Leges, 2017, s 107.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

očakávať nenarušanie súkromia zo strany tretích osôb z dôvodu vytvárania a udržovania sociálnych kontaktov alebo ide výlučne o výkon povolania, t.j. výlučne o pracovnú oblasť, v ktorej je očakávanie súkromia neopodstatnené.

7.5.2 Monitoring elektronickej komunikácie zamestnanca – prípad Barbulescu vs. Rumunsko

E-mailová a iná elektronická komunikácia patrí v súčasnosti medzi najčastejšie a najbežnejšie komunikačné kanály. Ako už bolo spomínané, tak čoraz viac je využívaná aj v pracovnom živote a pri plnení pracovných úloh zamestnancov. Zamestnávatelia samotní pokynujú zamestnancov k používaniu týchto masových komunikačných kanálov, čo im zväčša uľahčuje samotnú prácu, zvyšuje efektivitu pracovného výkonu a pod. Avšak na druhej strane vyvstáva do popredia otázka zneužívania komunikačných kanálov zamestnancami aj na inú komunikáciu ako pracovný a to v pracovnom čase. Zamestnávatelia tak čoraz väčšmi využívajú rôzne sledovacie aplikácie (softvér aj hardvér), ktorými sa snažia odkontrolovať správanie zamestnancov.

Do praktického stretu sa tak dostávajú dve ústavou garantované práva a to právo na ochranu súkromia zamestnanca v spojení s právom na ochranu osobných údajov a právom na ochranu vlastníctva zamestnávateľa.

7.5.2.1 Právo na ochranu súkromia

V prvom rade je potrebné poukázať na všeobecnú zásadu práva na súkromný život, ktoré je ako základné ľudské právo chránené najmä medzinárodnými dohovormi (Dohovor Rady Európy o ochrane ľudských práv a základných slobôd, Charty základných práv Európskej únie) a Ústavou SR. Nemožno opomenúť ani právo na ochranu osobnosti a ochranu pred neoprávnenými zásahmi do súkromnej sféry. V zmysle článku 16 ods. 1 Ústavy SR sa zaručuje nedotknuteľnosť osoby a jej súkromia. Obmedzená môže byť len v prípadoch ustanovených zákonom, ide o situácie týkajúce sa najmä oprávnení príslušníkov Policajného zboru, a podobne.

V súvislosti s ochranou osobnosti článok 19 ods. 2 Ústavy SR uvádza, že každý má právo na zachovanie ľudskej dôstojnosti, osobnej cti, dobrej povesti a na ochranu mena, každý má

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života a každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.

„Zosúladenie úpravy čl. 16 ods. 1 a čl. 19 ods. 2 Ústavy SR s medzinárodným štandardom ochrany práva na súkromie, ale aj so zdravým rozumom, predpokladá upustenie od doslovného výkladu čl. 16 ods. 1 a čl. 19 ods. 2 a jeho nahradenie extenzívnym výkladom vychádzajúcim z tézy, že čl. 16 ods. 1 a čl. 19 ods. 2 chránia hodnoty súkromnej povahy v jedinom a jednotnom systéme vytvorenom podľa požiadavky kompatibility s ochranou ľudského práva na súkromie.“[259] S rovnakým názorom sa stotožnil aj Ústavný súd SR, ktorý vo svojich judikátov prezentuje myšlienku jednotného systému ochrany súkromia fyzických osôb.[260]

„Ústava vo viacerých ustanoveniach dotvára jednotnú úpravu práva na súkromný život, ktorého podstatou je možnosť jednotlivca v určitej sfére spoločenských vzťahov žiť podľa svojich predstáv bez zbytočných obmedzení, príkazov a zákazov ustanovených orgánom verejnej moci. Ústavou vytvorená ochrana práva na súkromie sa vnútorne diferencuje. Jednotlivými ustanoveniami sa zaručuje ochrana súkromia v rôznych životných situáciách. Ústavný súd v súlade s tým vyslovil právny názor, podľa ktorého ochrana osobných údajov sa podľa čl. 22 ods. 1 Ústavy SR zaručuje iba v priamej súvislosti v listovým tajomstvom a tajomstvom dopravovaných správ.[261]

Ústavou zakotvené právo na súkromie a občianskoprávna ochrana osobnosti fyzickej osoby (zahŕňajúc aj právo na súkromie) sa častokrát stotožňuje avšak práve Ústavný súd SR túto polemiku vyvrátil vo svojom náleze z 15.10.1997 č. II. ÚS 59/97, keď uviedol že cit.: „Ústava spravidla zaručuje ochranu záujmov a hodnôt v spoločenských vzťahoch presahujúcich rozsah jedného právneho odvetvia. Ústavou zaručené právo na súkromie nie je identické s právom na súkromie, ktoré chráni Občiansky zákonník. Právo na súkromie podľa Občianskeho

[259] Drgonec, J.: Ústava Slovenskej republiky. Komentár. 3. vydanie. Šamorín: Heuréka, 2012, s. 329.
[260] K tomu pozri napr.: Nález Ústavného súdu SR PL ÚS 43/95. Nález z 10. septembra 1996. Zbierka nálezov a uznesení Ústavného súdu SR 1996, s. 144).
[261] Nález Ústavného súdu SR I. ÚS 33/95.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zákonníka nie je zanedbateľnou zložkou ústavného práva na súkromie. Ústavou zaručené právo na súkromie sa však napĺňa aj niektorými ustanoveniami Zákona o rodine. Ústavou zaručené právo na súkromie štát chráni aj v odvetví trestného práva vytvorením skutkových podstát trestných činov porušujúcich súkromie (porušovanie domovej slobody podľa §238 Trestného zákona, § 239 a 240 porušovanie tajomstva prepravovaných správ).“[262]

Ochrana súkromia je realizovaná aj v ďalšej oblasti právnej úpravy a to v pracovnom práve. V zmysle článku 11 tvoriaceho jednu zo základných zásad stanovených zákonom č. 311/2001 Z. z. Zákonníkom práce v platnom znení (ďalej len „Zákonník práce") zamestnávateľ môže o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával.

Právo na ochranu osobných údajov síce slovenský zákonodarca upravuje značne konkrétne, avšak v zmysle európskeho dohovoru o ochrane ľudských práv a základných slobôd ochrana osobných údajov koncepčne spadá do práva na ochranu súkromia. Zákonník práce však nijako nedefinuje, čo je možné považovať za predmet ochrany spadajúcej pod článok 11, a preto je potrebné použiť definíciu, tak ako ju stanovuje Zákon č. 122/2013 Z. z., ktorý v § 4 ods. 1 definuje osobné údaje ako „*údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu*.“[263] Napriek zákonom o ochrane osobných údajov vymedzenom pojme osobné údaje, „*pod pojmom osobné údaje judikatúra ESĽP rozumie všetky informácie o určitej alebo určiteľnej osobe. O určiteľnú osoby ide vtedy, ak ju možno priamo alebo nepriamo identifikovať na základe určitého kľúča (napr. rodné číslo, údaje o zdraví)*.“[264] Osobným údajom je v súčasnosti aj IP adresa užívateľa internetového pripojenia.

[262] Nález Ústavného súdu SR z 15.10.1997 sp. zn. II. ÚS 59/97. Zbierka nálezov a uznesení Ústavného súdu Slovenskej republiky 1997, s. 290-291.
[263] § 4 ods. 1 zákona o ochrane osobných údajov.
[264] Barancová, H. Zákonník práce. Komentár 4. vydanie. Bratislava : C.H. Beck, 2015, s. 99.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Ako sme už uviedli, tak právo na ochranu osobných údajov sa z obsahového hľadiska považuje za právo patriace do práva na ochranu súkromia. Čl. 11 ZP tak môžeme považovať za základný právny rámec rozsahu zásahu do súkromia zamestnanca zo strany zamestnávateľa, keď ZP v čl. 11 vymedzuje rozsah osobných údajov, ktoré môže zamestnávateľ zhromažďovať.

Zákonník práce sa v článku 11 obmedzuje na zákonnú limitáciu oprávnenia zamestnávateľa zhromažďovať dva druhy údajov; osobné údaje o zamestnancovi a iné údaje o zamestnancovi, ktoré síce nemusia mať v zmysle zákona o ochrane osobných údajov povahu osobných údajov, ktoré môžu mať význam z hľadiska vykonávanej práce zamestnanca alebo z hľadiska práce, ktorú má vykonávať, vykonáva alebo ktorú vykonával.

Vyslovene, je právo na ochranu súkromia zamestnancov chránené priamo v paragrafovom znení Zákonníka práce, a to konkrétne v § 13 ods. 4 ZP, ktorý znie, cit.: „*Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje, vykonáva záznam telefonických hovorov uskutočňovaných technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronickú poštu odoslanú z pracovnej elektronickej adresy a doručenú na túto adresu bez toho, aby ho na to vopred upozornil. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.*“[265]

Samotné právo na súkromie zamestnanca resp. právo na ochranu súkromného života zamestnanca a pod. je chránené nie absolútne ale relatívne, čo znamená, že „*sú obmedziteľné, a to za predpokladu, že ich obmedzenie prejde tzv. ústavným testom proporcionality, ktorý spravidla predvída sama ústava. ... Test proporcionality by sa dal charakterizovať aj ako séria krokov (subtestov), ktoré musia byť naplnené, aby mohlo prísť k ústavnému obmedzeniu ľudského práva alebo základnej slobody*.“[266] Základným pravidlom pri zásahu zamestnávateľa

[265] § 13 ods. 4 Zákonníka práce.
[266] Ľalík, T.: Úvod do problematiky ľudských práv. In: Ústavné právo. - ISBN 978-80-8168-511-8. - Bratislava : Wolters Kluwer, 2016. S. 285.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

do zamestnancových práv na súkromie, čo sa týka rozsahu tohto zásahu, je tak limitácia z hľadiska toho, že tieto zásahy je možné vykonávať iba medziach zásad legality, legitimity a proporcionality (spomínaný test proporcionality), v zmysle ktorých bude monitoring zamestnanca zákonný len vtedy, ak takúto kontrolu zákon predpokladá a bude uskutočnená iba v zákonom predvídanom rozsahu a miere.

§ 13 ods. 4 ZP tak predstavuje právny rámec na tzv. monitoring zamestnancov zamestnávateľom, tzn. monitorovanie e-mailovej korešpondencie, teda elektronickej pošty, záznam telefonických hovorov, ale v intenciách judikatúry ESĽP sa tieto možnosti monitoringu vzťahujú nielen na zákonom vymedzené možnosti, ale pridávajú sa k nim aj ďalšie možnosti, ako napríklad monitoring pohybu zamestnancov na motorovom vozidle zamestnávateľa a pod.

Samotný monitoring zamestnancov je dovolený, avšak podmienený splnením viacerých povinností.

Týmito podmienkami sú:

- Zamestnávateľ má na to vážny dôvod, ktorý spočíva v osobitnej povahe vykonávanej práce zamestnancom, resp. osobitnej povahe zamestnávateľa, a
- Ide o zásah do súkromia zamestnanca, ktorý spočíva v monitorovaní zamestnanca pri plnení pracovných úloh v pracovnom čase a v zásade na pracovisku (iné miesto nevylučujúc, napr. pri pracovnej ceste).

ZP nevymedzuje v § 13 ods. 4 všetky spôsoby monitorovania zamestnancov, „z čoho vyplýva, že zamestnávateľ j oprávnený, ak splní zákonné podmienky § 13 ods. 4 ZP vykonávať aj také konkrétne formy monitorovania zamestnancov, ktoré nie sú uvedené v § 13 ZP. Ide predovšetkým o videokamery na pracovisku (nevylučujúc zaznamenávanie polohy služobného motorového vozidla používaného zamestnancom a pod., pozn. autora).[267]

Monitorovanie zamestnancov je legitímne iba v prípade, ak zamestnávateľ splní svoju oznamovaciu povinnosť voči zamestnancovi a vopred ho upovedomí o existencii kontroly,

[267] Barancová, H. Zákonník práce. Komentár 4. vydanie. Bratislava : C.H. Beck, 2015, s. 250.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

rozsahu kontroly a o forme a spôsobe vykonávania kontroly. Zásada proporcionality bude dodržaná, ak sa kontrola uskutoční len v nevyhnutnej miere, napríklad za účelom dodržania ochrany zdravia pri práci a nebude tým porušená ľudská dôstojnosť zamestnanca.

Vážne dôvody tak, ako sú vyššie uvedené, sa v každom prípade v závislosti od charakteru práce, miesta práce a podobne, posudzujú individuálne.

Vážne dôvody je aj v prípade sledovania elektronickej pošty potrebné posudzovať individuálne vzhľadom na predmet a činnosť zamestnávateľa, napríklad je odlišné posudzovanie dôvodov sledovania elektronickej pošty zamestnávateľom, ktorý je softvérovou spoločnosťou a vyrába antivírusové programy a odlišné u zamestnávateľa, ktorého predmet činnosti sú napríklad sťahovacie služby. Rovnako relevantným subjektívnym prvkom je aj druh práce, ktorú zamestnanec vykonáva. V tomto prípade je rozdiel, keď je zamestnanec IT-technik alebo upratovačka. Najviac v praxi využívaným „vážnym“ dôvodom pre zamestnávateľa je ochrana majetku zamestnávateľa. Právo na ochranu majetku má zamestnávateľ nielen v zmysle § 13 ods. 4 ZP ale aj § 177 ods. 2 ZP, ktorý znie: „*Na ochranu svojho majetku je zamestnávateľ oprávnený vykonávať v nevyhnutnom rozsahu kontrolu vecí, ktoré zamestnanci vnášajú na pracovisko alebo odnášajú z pracoviska. Podrobnejšie podmienky určí zamestnávateľ v pracovnom poriadku. Pri kontrole sa musia dodržať predpisy o ochrane osobnej slobody a nesmie byť ponižovaná ľudská dôstojnosť*.“[268]

V praxi nie je výnimkou realizácia monitoringu telefonických hovorov zamestnancov s cieľom prevencie pred vybavovaním súkromných hovorov zamestnancov zo služobných zariadení. Pri monitorovaní telefonických hovorov musí byť dodržaná ochrana súkromia, obsah telefonátov musí ostať v utajení. Zamestnávateľ nemôže odpočúvať telefónne hovory, môže len zistiť volané čísla.

Zamestnávateľ môže vo svojom vnútornom predpise upraviť používanie elektronickej pošty, sledovania telefonických hovorov alebo vyhotovovania kamerových záznamov zamestnancov, avšak za predpokladu, že splní vyššie uvedené podmienky. Vnútorný predpis, ktorý dovoľuje monitoring zamestnancov, sám o sebe nelegitimizuje samotný monitoring, je len

[268] § 177 ods. 2 ZP.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

predpokladom pre samotnú realizáciu monitoringu za splnenie zákonom stanovených podmienok. Úprava monitoringu vo vnútornom predpise zamestnávateľa len napĺňa jednu z podmienok monitoringu, a t.j., že zamestnanec má právo byť o kontrole informovaný spolu so všetkými podmienkami príslušného monitoringu a zároveň je povinnosťou zamestnávateľa, aby o uvedenom zamestnanca informoval a poučil.

7.5.2.2 Analýza jednotlivých rozhodnutí v prípade Barbulescu vs. Rumunsko

Keďže právna úprava monitoringu zamestnancov zamestnávateľmi nie je veľmi konkrétna a rozpracovaná, a častokrát sa tak zamestnávateľ pri realizácii monitoringu, ako aj zamestnanec dostávajú do problémových situácií, tak čoraz väčšmi nielen odborníci z akademickej obce ale aj prax samotná privítajú ak nejaká súdna inštancia príjme v spornej veci rozhodnutie, resp. vysloví svoj názor a tým odstráni pochybnosti pri aplikácií právnej úpravy na praktické situácie. Jedným z takýchto rozhodnutí je rozhodnutie Európskeho súdu pre ľudské práva (ďalej len „ESĽP"), ktorý rozhodoval vo veci Barbulescu vs. Rumunsko.

7.5.2.3 Prvé rozhodnutie

Európsky súd pre ľudské práva vydal 12.1.2016 rozhodnutie v spore Barbulescu proti Rumunsku, v ktorom išlo najmä o ochranu súkromia zamestnanca na pracovisku (ďalej len „prvé rozhodnutie").

V prípade „Barbulescu" v podstate išlo o sledovanie (monitoring) zamestnanca zamestnávateľom na pracovisku s tým, že zamestnávateľ sledoval „chatovaciu" komunikáciu zamestnanca prostredníctvom program Yahoo Messenger. Zamestnanec mal túto chatovaciu linku používať na pracovné účely a to na komunikáciu s klientmi. Zamestnanec však v pracovnom čase toto chatovanie realizoval nielen na komunikáciu s klientmi, ale aj s priateľkou a bratom. Zamesntávateľ však prostredníctvom sledovacieho softvéru zaznamenával komunikáciu zamestnanca na pracovisku a v pracovnom čase so súkromnými osobami, načo ho asi po týždni monitoringu konfrontoval s jeho výsledkami. Výsledkom konfrontácie bolo skončenie pracovného pomeru so zamestnancom okamžite a to za používanie internetu a pracovného chatu v pracovnej dobe na súkromné účely.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Po vyčerpaní všetkých vnútroštátnych možností na súdnu ochranu sa zamestnanec obrátil na ESĽP, na ktorom sa domáhal toho, že Rumunsko, ako signatár Európskej dohody o ochrane ľudských práv a základných slobôd porušilo čl. 8 ods. 1 tejto dohody, ktorý zaručuje každému právo na rešpektovanie súkromného a rodinného života.

ESĽP po ťažkom rozhodovaní nakoniec pripustil, že zamestnávateľ bol oprávnený sledovať konverzácie zamestnanca na Yahoo Messengeri na to, aby zistil, či sa v pracovnom čase venuje práci.

Právnou vetou, na ktorej ESĽP postavilo obhajobu zamestnávateľovho postupu bolo to, že na to, aby sa zistilo, či je monitorovanie zamestnanca, teda napríklad nahrávanie jeho hovorov, sledovanie jeho činnosti na internete alebo telefonických hovorov v rozpore s čl. 8 Európskej dohody o ochrane ľudských práv a základných slobôd je potrebné skúmať, či zamestnanec mohol alebo nemohol pri svojej súkromnej komunikácii odôvodnene očakávať súkromie alebo nie.

„Európsky súd pre ľudské práva vo svojom rozsudku konštatoval, že nepovažuje za neprimerané, že si zamestnávateľ chcel overiť, či zamestnanci počas pracovného času plnia svoje pracovné povinnosti, a že zamestnávateľ vstúpil do účtu sťažovateľa v domnienke, že tento obsahuje komunikáciu týkajúcu sa klientov. Ďalej poukázal na to, že v konaní pred vnútroštátnymi súdmi mal sťažovateľ možnosť uplatniť argumenty o údajnom porušení jeho práva na rešpektovanie súkromia a korešpondencie, pričom v rozhodnutiach vydaných týmito súdmi nie je zmienka o obsahu jeho komunikácie. Pred súdmi bol prepis tejto komunikácie využitý iba v rozsahu nevyhnutnom na preukázanie, že využíval firemný počítač počas pracovného času na súkromné účely, avšak identita ľudí, s ktorými komunikoval, nebola sprístupnená. Zamestnávateľ okrem toho monitoroval len Yahoo Messenger konto, nie iný obsah sťažovateľovho počítača. Na základe uvedeného európsky súd dospel k záveru, že vnútroštátne súdy pri posudzovaní veci dodržali spravodlivú rovnováhu medzi právom sťažovateľa na ochrane súkromia a korešpondencie a záujmami jeho zamestnávateľa.“[269]

[269] Tlačová správa Ministerstva spravodlivosti vo veci Bărbulescu proti Rumunsku z 12. januára 2016. Dostupná k 10.12.2017 na https://www.justice.gov.sk/Stranky/aktualitadetail.aspx?announcementID=2048.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

V každom takom prípade, resp. pri kontrole legitimity a legality monitoringu zamestnanca sa zisťuje najmä, či zamestnávateľ uložil zamestnancom nejaké vnútorné pravidlá a pokyny na používanie elektronickej komunikácie, výpočtovej techniky a telefónov a je potrebné preskúmať aj bežnú prax na danom pracovisku. Uvedené znamená, či zamestnávateľ informoval zamestnanca o možnom resp. reálnom monitoringu na pracovisku.

Z uvedeného rozhodnutia ESĽP z roku 2016 však vyplýva, že na to, aby zamestnávateľ mohol monitorovať svojich zamestnancov postačí, ak možno zo strany zamestnanca odôvodnene očakávať monitoring. V zmysle uvedené tak nie je nutné zo strany zamestnávateľa informovať zamestnanca, že dochádza k monitoringu.

V roku 2016 tento rozsudok ESĽP vyvolal veľkú mieru rozruchu a to tak v odborných ako aj laických kruhov, nakoľko v podstate legitimoval právo zamestnávateľa na monitoring zamestnancov bez ich predchádzajúceho súhlasu.

V tomto prípade bolo sporné, či zamestnávateľ Barbulesca informoval o tom, že jeho chaty môže monitorovať. Zamestnávateľ predložil súdu svoje vnútorné predpisy o sledovaní elektronickej komunikácie, ktoré vydal asi týždeň pred začatím sledovania, chýbal pri nich ale Barbulescov podpis, ktorý by dosvedčil, že Barbulescu o takom predpise vedel. Barbulescu sa pre Európskym súdom bránil, že zo samotnej povahy chatu vyplýva, že ide o súkromnú konverzáciu a preto sledovanie zo strany zamestnávateľa nemohol očakávať. Tiež tvrdil, že síce zamestnávateľ používanie počítačov na súkromné účely vo svojich predpisoch zakázal, ale neuviedol tam, že by mohol zamestnancov sledovať, aby zistil, či zákaz dodržiavajú. Nariadenie, ktoré umožňovalo sledovanie, podľa neho vyprodukoval zamestnávateľ až ex post a Barbulescu o ňom v čase sledovania nevedel. Súd všetko zvážil a konštatoval, že do zásahu do Barbulescovho súkromia skutočne došlo. Potom ale posudzoval, či bol tento zásah oprávnený a primeraný, pretože nie je nedôvodné aby zamestnávateľ kontroloval, či jeho zamestnanci v práci skutočne pracujú. Sledovanie v danom prípade trvalo iba týždeň a nezistilo sa, že by zamestnávateľ pristupoval inak do počítača zamestnancov alebo kontroval nejaké iné súbory. Súd napokon skonštatoval, že v danom prípade bol zásah do Barbulescovho súkromia primeraný a dostatočne obmedzený. Preto súd rozhodol, že Barbulescove práva podľa čl. 8

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

dohody neboli porušené. Nešťastný Barbulescu teda ostal bez práce a my ostatní sme zistili, že právo zamestnanca na súkromie v práci je rozhodne obmedzené.

Ak by bol Barbulescu zamestnaný na Slovensku a k prípadu došlo by teraz, mal by zrejme v spore so zamestnávateľom o niečo lepšie postavenie. Zákonník práce platný pre slovenských zamestnávateľov totiž pomerne podrobne (aj keď nie veľmi presne) určuje pravidlá pre zamestnávateľov, ktoré musia dodržať, ak chcú zamestnancov v práci sledovať.

7.5.2.4 Rozhodnutie pred Veľkou komorou a rozhodnutie zo dňa 5.9.2017

Podniky musia vopred varovať svojich zamestnancov, že ich elektronická komunikácia je monitorovaná, čo sa v Rumunsku nestalo.

Či zistil súd, prečo si myslí, že bol porušený čl. 8 Dohovoru:

- Rumunské súdy zle posúdili rovnováhu medzi záujmami Barbulescua a jeho zamestnávateľa na hladkom chode spoločnosti.
- Takisto súd dospel k záverom, že rumunské súdy neposúdili otázku, či bol barbulescu informovaný o monitorovaní o rozsahu, spôsobe, dôvodoch, či bolo možné ochranu zamestnávateľa dosiahnuť aj iným spôsobom, a po tretie či komunikácia barbulescua mohla byť dostupná aj bez jeho vedomia tretim stranám.

Čo znamená nové rozhodnutie v tejto veci?

- Neznamená to, že by zamestnávatelia nemohli monitorovať za žiadnych okolností svojich zamestnancov v práci, avšak je potrebné prijať opatrenia na zabezpečenie toho, aby nedošlo k porušovaniu práva na súkromie.
- Súd vyšpecifikoval kritéria je potrebné dodržať aby sa dodržala miera vyváženosti medzi záujmami oboch strán sporu a nedošlo k neprimeranému zásahu do práva na súkromie:

a) Zamestnávateľ musí zamestnanca informovať o možnosti monitorovania. Informácia by mala byť jasná a dostatočne špecifická, aby bolo z nej možné zistiť ako, kedy a v akom rozsahu je zamestnanec monitorovaný,

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

b) Pri posudzovaní primeranosti by sa malo posudzovať, či bol monitorovaný iba tok informácií alebo aj samotný obsah, či sa monitorovala všetka komunikácia alebo iba časť z nich, či bolo monitorovanie neobmedzené alebo časovo ohraničené a to, či k výsledkom monitorovania mal prístup aj tretí subjekt a v akom rozsahu.

c) V oveľa väčšej miere by sa mali súdy zaoberať otázkou sily zamestnávateľovho odôvodnenia v závislosti od toho, či sa sledoval iba tok informácií alebo aj ich obsah. Ak obsah, tak je potrebné silnejšie odôvodnenie.

d) Ďalej je potrebné skúmať či by bolo možné vytvoriť monitorovací systém založený na menej rušivých metódach a opatreniach ako priamo pristupovať k obsahu komunikácie zamestnanca. Z hľadiska konkrétnych okolností každého prípadu by sa malo posúdiť, či cieľ sledovaný zamestnávateľom by sa mohol dosiahnuť bez priameho úplného prístupu k obsahu komunikácie zamestnanca;

e) či boli výsledky monitorovania použité k uvádzanému účelu a splnili účel.

f) či zamestnancovi boli poskytnuté primerané záruky, najmä ak monitorovacie operácie zamestnávateľa majú narušujúci charakter. Takéto záruky by mali byť najmä zabezpečenie, aby zamestnávateľ nemal prístup k skutočnému obsahu príslušnej komunikácie.

Dvor audítorov po prvýkrát preskúmal prípad týkajúci sa monitorovania zamestnanca elektronická komunikácia súkromným zamestnávateľom. Vo veci **Copland proti Veľkej Británii** (č. 62617/00) Súd dospel k záveru, že došlo k porušeniu článku 8 dohovoru z dôvodu, že sledovanie telefonickej komunikácie žiadateľa, používanie elektronickej pošty a internetu nebolo "v súlade so zákonom ", keďže v príslušnom čase neexistovalo žiadne vnútroštátne právo na reguláciu monitoringu. Dvor audítorov okrem toho rozhodol o značnom počte prípadov týkajúcich sa sledovanie telefónnych komunikácií alebo zhabanie elektronických údajov štátnymi orgánmi v kontexte presadzovania práva alebo ochrany národnej bezpečnosti.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Súd skúma žiadosti, ktoré mu boli predložené na individuálnom základe. Avšak é členské štáty vyvodzujú potrebné dôsledky z rozsudku Súdneho dvora a mali by svoje práva zosúladiť, aby sa vyhli zisteniam o podobných porušeniach európskeho práva.

Vo svojom rozsudku vo veci Bărbulescu proti Rumunsku Súdny dvor upresňuje kritériá, ktoré majú uplatňovať vnútroštátne orgány pri posudzovaní toho, či opatrenie na monitorovanie komunikácie zamestnancov je primerané sledovanému cieľu a či zamestnanec je chránený pred svojvoľnosťou.

7.5.2.5 Prípad Barbulescu v judikatúre Najvyššieho súdu Slovenskej republiky

Jedným z prvých odznení rozsudkov Bărbulescu je slovenský prípad vo verejnom sektore. Ministerstvo vnútra Slovenskej republiky v roku 2011 disciplinárne prepustilo zamestnanca za používanie služobnej e-mailovej adresy v osobný prospech, čo nebolo povolené. V tom období neexistoval jasná vnútroštátna úprava týkajúci sa tejto otázky a to ani v Zákonníku práce účinného v tom čase vrátane predchádzajúceho zákona o štátnej službe.

Najvyšší súd Slovenskej republiky[270], prihliadajúc na príslušné medzinárodné a ústavné normy ako legálnosť, legitimitu a proporcionalitu, rozhodol, že súdy nižších inštancií mali pravdu v tom, že zamestnávateľ mal plné právo skontrolovať e-maily zamestnanca a na základe týchto dôkazov rozhodnúť. Potvrdil rozhodnutie o prepustení so zdôvodnením, že správanie zamestnanca bolo nevhodné.

Zaujímavé je, že Najvyšší súd nevyžadoval predchádzajúce upozornenie o možnosti monitorovania komunikácie zo strany zamestnávateľa. Na odôvodnenie svojho rozhodnutia sa odvolal na prvý rozsudok komory Európskeho súdu pre ľudské práva v prípade Bărbulescu v prospech zamestnávateľa, aj keď konanie stále prebiehalo pred veľkou komorou Európskeho súdu pre ľudské práva. Neskôr Ústavný súd Slovenskej republiky zamietol sťažnosť zamestnanca.[271]

[270] Rozsudok NS SR z 12.09.2016, sp. zn. 3Cdo/233/2015.
[271] Ústavný súd Slovenskej republiky, sp. zn. IV. ÚS 254/2018-10.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

8 PRÁVNE PROSTRIEDKY OCHRANY PRED NEZÁKONNÝM ZÁSAHOM DO SÚKROMIA ZAMESTNANCA

8.1 VŠEOBECNÉ VYMEDZENIE PRACOVNOPRÁVNYCH SPOROV

Spory v pracovnom práve nie sú ojedinelým úkazom. V zásade platí, že spory vznikajú vo všetkých právnych vzťahoch rôznych právnych odvetví, pričom pracovné právo, resp. pracovnoprávne vzťahy nie sú výnimkou. Vychádzajúc z definície pracovnoprávnych vzťahov ako právnych vzťahov, v ktorých účastníci vystupujú ako nositelia subjektívnych práv a právnych povinností všeobecne ustanovených a zabezpečených normami pracovného práva[272], je možné konštatovať, že spory v týchto vzťahoch vznikajú tým, že tieto subjekty porušujú tieto práva, alebo nedodržiavajú svoje povinnosti. Keďže z hľadiska predmetu rozdeľujeme pracovnoprávne vzťahy na individuálne a kolektívne, tak prirodzene aj spory, ktoré v týchto vzťahoch vznikajú delíme na spory individuálne a spory kolektívne. V tejto časti sa budeme zaoberať problematikou individuálnych pracovných sporov. Všeobecne platí, že realizácia subjektívnych práv a právnych povinností v pracovnoprávnych vzťahoch je jednou z najdôležitejších foriem realizácie práva. Pri tejto realizácii často krát dochádza k prekročeniu ustanovených oprávnení a tým aj k zneužitiu práva ako takého. Vychádzajúc zo základných zásad zákona č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov (ďalej len „Zákonník práce“) v čl. 2 síce vyplýva, že *„výkon práv a povinností vyplývajúcich z pracovnoprávnych vzťahov musí byť v súlade s dobrými mravmi; nikto nesmie tieto práva a povinnosti zneužívať na škodu druhého účastníka pracovnoprávneho vzťahu alebo spoluzamestnancov“*, ale aj napriek tomu k zneužívaniu práva dochádza. Pracovné právo ako samostatné odvetvie právneho poriadku, počíta aj s touto situáciou a upravuje vo svojich normách niekoľko postupov na riešenie vzniknutých sporov[273]. Na druhej strane je však potrebné podčiarknuť zásadnú skutočnosť, že v rámci osobitnej úpravy riešenia individuálnych pracovných sporov je pracovné právo deficitné a „spolieha“ sa na základnú normu občianskeho práva procesného. Úprava spôsobov riešenia sporov z pracovnoprávnych

[272] BARANCOVÁ, H. SCHRONK, R. Pracovné právo, Bratislava SPRINT 2007, ISBN: 978-80-89085-95- 8, s. 197
[273] K tomu pozri bližšie aj KURIL, M. Procesná autonómnosť pracovného práva - quo vadis? In: KURIL. M. *Zákon č. 311/2001 Z.z. Zákonník práce desať rokov aplikačnej praxe (2001-2011)* : zborník vedeckých článkov – 1. vyd. – Bratislava : Právnická fakulta, 2012 – 167 s. ISBN 978-80-7160-327-6.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

vzťahov spadá obsahovo pod ochrannú funkciu pracovného práva. Nemusíme sa strániť poukázať aj na fakt, že k zneužívaniu práv dochádza vo väčšej miere v neprospech „slabšieho" účastníka pracovnoprávneho vzťahu – zamestnanca. Pracovné právo teda nevyhnutne musí prinášať nielen spôsoby riešenia už vzniknutých sporov, ale vytvárať najmä také právne prostredie, aby k sporom nedochádzalo. Istý rámec už bol naznačený v rámci ustanovení základných zásad, no ochrana oprávnených záujmov subjektov pracovnoprávnych vzťahov sa prelína celým právnym odvetvím. Ak sa na túto problematiku pozrieme optikou základného pracovnoprávneho predpisu, tak môžeme skonštatovať, že Zákonník práce definuje niekoľko spôsobov ochrany práv a oprávnených záujmov týchto subjektov. Základný kameň riešenia sporov ustanovuje Zákonník práce v čl. 9 základných zásad *(„Zamestnanci a zamestnávatelia, ktorí sú poškodení porušením povinností vyplývajúcich z pracovnoprávnych vzťahov, môžu svoje práva uplatniť na súde. Zamestnávatelia nesmú znevýhodňovať a poškodzovať zamestnancov preto, že zamestnanci uplatňujú svoje práva vyplývajúce z pracovnoprávnych vzťahov")* v spojitosti s normatívnym ustanovením § 14, ktorý konštatuje, že *„spory medzi zamestnancom a zamestnávateľom o nároky z pracovnoprávnych vzťahov prejednávajú a rozhodujú súdy".* Ostatné spory (teda iné ako spory o nároky) je možné riešiť aj inými spôsobmi. Tie si rozoberieme v nasledujúcom texte.

V súvislosti s porušovaním pracovnoprávnych zo strany zamestnávateľa predpisov na úseku ochrany súkromia zamestnancov je potrebné sa zmieniť o prostriedkoch právnej ochrany zamestnancov. Prostriedky právnej ochrany zamestnancov priamo súvisia s ochrannou funkciou pracovného práva. Ochranná funkcia pracovného práva sa okrem iného premieta aj do prostriedkov právnej ochrany slúžiacich na ochranu ohrozených alebo porušených práv zamestnancov. Výnimkou v tomto smere nie je ani porušenie alebo ohrozenie práva na súkromie zamestnancov na pracovisku zamestnávateľa. Je tomu tak preto, pretože zamestnanec je v rámci pracovnoprávneho vzťahu slabšou zmluvnou stranou oproti zamestnávateľovi. Z uvedeného dôvodu pri vybraných právach zamestnancov Zákonník práce spája s ich porušením právo zamestnanca na ich právnu ochranu. Právne prostriedky ochrany porušeného alebo ohrozeného práva na súkromie zamestnanca možno rozdeliť z viacerých

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

hľadísk. Z hľadiska subjektu poskytujúceho právnu ochranu zamestnancom možno právne prostriedky garancie ochrany práva na súkromie rozdeliť na:

a) právna ochrana poskytnutá zamestnávateľom;

b) právna ochrana poskytnutá zástupcami zamestnancov;

c) právna ochrana poskytnutá orgánmi verejnej moci;

d) právna ochrana poskytnutá mimosúdnou cestou;

e) právna ochrana poskytnutá súdnou cestou.

Z hľadiska právnych prostriedkov patriacich zamestnancom, ktoré môžu efektívne využiť na ochranu ohrozeného alebo porušeného práva na súkromie, môžeme zaradiť napríklad:

a) sťažnosť zamestnanca zamestnávateľovi;

b) podnet zamestnanca zástupcom zamestnancov alebo orgánu inšpekcie práce;

c) uzatvorenie dohody o začatí mediácie;

d) podanie žaloby na príslušný súd;

e) návrh na začatie trestného alebo priestupkového konania;

f) oznámenie o kriminalite alebo inej protispoločenskej činnosti.

8.2 PRÁVNA OCHRANA PROSTREDNÍCTVOM ZAMESTNÁVATEĽA

Právna ochrana zamestnanca poskytnutá od svojho zamestnávateľa patrí k základným právam zamestnanca, ktorá mu vyplýva z pracovnoprávneho vzťahu. Právna ochrana zamestnanca, ktorá je poskytovaná od zamestnávateľa, sa realizuje najmä prostredníctvom inštitútu sťažnosti.

Sťažnosť zamestnanca patrí k najvšeobecnejším právnym prostriedkom nápravy ohrozených alebo porušených práv zamestnanca. Právo zamestnanca na podanie sťažnosti zamestnávateľovi je upravené najmä v § 13 Zákonníka práce. Podľa § 13 ods. 7 Zákonníka práce má zamestnanec právo podať zamestnávateľovi sťažnosť v prípade:

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

a) porušenia zásady rovnakého zaobchádzania (§ 13 ods. 1 Zákonníka práce),

b) porušenia zákazu diskriminácie (13 ods. 2 Zákonníka práce),

c) výkonu práva a povinností v rozpore s dobrými mravmi (§ 13 ods. 3 Zákonníka práce),

d) neoprávneného narušenia súkromia zamestnanca (§ 13 ods. 4 Zákonníka práce),

e) neoprávnenému uloženiu povinnosti zachovávať mlčanlivosť (§ 13 ods. 5 Zákonníka práce),

f) neoprávnený zákaz výkonu inej zárobkovej činnosti (§ 13 ods. 6 Zákonníka práce),

g) porušenia práv a povinností vyplývajúcich z pracovnoprávneho vzťahu.

Z uvedeného ustanovenia § 13 ods. 7 Zákonníka práce vyplýva, že zamestnanec je oprávnený podať zamestnávateľovi sťažnosť aj v prípade ohrozeného alebo porušeného práva na ochranu súkromia zamestnanca,. Je nutné podotknúť, že takého porušenie práva zamestnanca alebo povinnosť zamestnávateľa nemusí nutne vyplývať len z príslušných ustanovení Zákonníka práce upravujúcich ochranu súkromia zamestnanca na pracovisku, ale môže vyplývať aj z osobitných právnych predpisov upravujúcich právo na ochranu súkromia zamestnanca. Typickým príkladom je zákon na ochranu osobných údajov.

Adresátom sťažnosti je samotný zamestnávateľ. Z hľadiska pasívne legitimovaného subjektu sťažnosť bude smerovať voči narušiteľovi práva na ochranu súkromia zamestnanca, ktorým môže byť sám zamestnávateľ zamestnanca, užívateľský zamestnávateľ zamestnanca, druhý zamestnanec zamestnávateľa alebo inakší tretí subjekt ako napríklad súkromná bezpečnostná služba v právnom postavení obchodného partnera k zamestnávateľovi dotknutého zamestnanca. Sme toho názoru, že uvedené právo zamestnanca nepatrí zamestnancovi v rámci predzmluvných vzťahov, v rámci ktorých rovnako tak môže dochádzať k monitorovaniu zamestnancov, a to napríklad podrobením analýzy písaného písma uchádzača o zamestnanie grafológom a ďalšími odborníkmi, ktorí o uchádzačovi o zamestnanie vypracujú podrobnú správu, ktorá je určená pre potreby zamestnávateľa, a to všetko bez vedomosti uchádzača o zamestnanie. Nie je vylúčené ani to, že sťažnosť bude

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

smerovať voči neidentifikovanému subjektu a teda vo svojej podstate sa bude jednať o sťažnosť zamestnanca vo veci porušenia práva na ochranu súkromia. Sťažnosť zamestnanca môže mať podobu aj anonymnej sťažnosti bez konkrétneho mena zamestnanca. Úlohou zamestnávateľa v tomto prípade je, aby sám preveril a vyhodnotil, či uvedená sťažnosť je sťažnosťou jeho zamestnanca, čo môže byť v aplikačnej praxi veľmi problematické a zamestnávatelia z dôvodu právnej istoty aj takúto sťažnosť preverujú po obsahovej stránke. Zo sťažnosti zamestnanca rovnako tak môže vyplývať, že si zamestnanec sťažovateľ neželá, aby jeho totožnosť zamestnávateľ pred druhým zamestnancom odhalil alebo zverejnil, ale jeho totožnosť je v samotnej sťažnosti uvedená. V tomto prípade z dôvodu právnej istoty možno odporučiť, aby zamestnávatelia po zvážení obsahu sťažnosti a jej potencionálnych citlivých informácií rešpektovali právo na súkromie zamestnanca, ktorý samotnú sťažnosť voči druhému zamestnancovi podal z dôvodu narušenia súkromia iného zamestnanca. V takomto prípade musí zamestnávateľ chrániť právo na ochranu súkromia, integrity a totožnosti zamestnanca v právnom postavení podávateľa sťažnosti pred negatívnymi dôsledkami na pracovisku v prípade zverejnenia jeho totožnosti proti jeho vôli zamestnancovi, voči ktorému sťažnosť smeruje a ktorý sa na totožnosť podávateľa sťažnosti u zamestnávateľa dopytuje.

Zákonník práce neupravuje formou sťažnosti alebo jej podstatné náležitosti. Sťažnosť zamestnanec môže podať ústne alebo písomne zamestnávateľovi. Z hľadiska právnej istoty a garancie jej správneho vyriešenia možno odporučiť jej podanie v písomnej forme a jej zaslanie takým spôsobom, ktorý hodnoverným spôsobom bude preukazovať jej odoslanie a doručenie zamestnávateľovi. Z hľadiska obsahu je potrebné, aby zo sťažnosti vyplývalo:

a) kto ju podáva,

b) komu je sťažnosť určená,

c) identifikácia ohrozeného alebo porušeného práva zamestnanca,

d) čoho sa zamestnanec domáha,

e) dátum a podpis zamestnanca,

f) prípadné pripojenie príloh na preukázanie tvrdení zamestnanca.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Nakoľko však Zákonník práce neobsahuje výpočet náležitostí takejto sťažnosti, absencia niektorej z nich nebude mať za následok neplatnosť sťažnosti alebo jej nevybavenie zo strany zamestnávateľa. V prípade, že bola podaná zamestnávateľovi anonymná sťažnosť, z ktorej vôbec nevyplýva ani to, či ju podal jeho zamestnanec, zastávame právny názor, že zamestnávateľ by mal informácie v nej prešetriť, avšak nemusí striktne dodržať ustanovenie § 13 ods. 7 Zákonníka práce, napríklad v prípade písomnej odpovede zamestnancovi, keďže jeho totožnosť nie je zamestnávateľovi známa.

Podľa § 13 ods. 7 Zákonníka práce zamestnávateľ je povinný na sťažnosť zamestnanca bez zbytočného odkladu písomne odpovedať, vykonať nápravu, upustiť od takého konania a odstrániť jeho následky. Z uvedeného vyplýva, že Zákonník práce stanovuje pre odpoveď zamestnávateľa na sťažnosť zamestnanca písomnú formu. Písomná odpoveď zamestnávateľa je jeho právnym úkonom a keďže v zmysle § 17 ods. 2 Zákonníka práce chýba pri tomto ustanovení Zákonníka práce tzv. doložka neplatnosti, ústna odpoveď zamestnávateľa zamestnancovi na pracovisku bude platným právnym úkonom. Zamestnávateľ je povinný vykonať nápravu, pokiaľ stále pretrváva ohrozenie alebo porušenie práva na ochranu súkromia zamestnanca, je zamestnávateľ povinný upustiť od takéhoto konania a odstrániť jeho faktické a právne následky.

Podľa § 13 ods. 8 Zákonníka práce zamestnanec nesmie byť v pracovnoprávnom vzťahu prenasledovaný ani inak postihovaný za to, že podá na iného zamestnanca alebo na zamestnávateľa sťažnosť, podnet na príslušnom orgáne inšpekcie práce, žalobu, návrh na začatie trestného stíhania alebo iné oznámenie o kriminalite alebo inej protispoločenskej činnosti, nezachová mlčanlivosť o svojich pracovných podmienkach vrátane mzdových podmienok a o podmienkach zamestnávania alebo že si uplatňuje práva a právom chránené záujmy vyplývajúce z pracovnoprávneho vzťahu. Pokiaľ ohrozenie alebo porušenie práva na ochranu súkromia zamestnanca na pracovisku zamestnávateľa stále trvá a zamestnávateľ po dlhší čas nečinný.

V aplikačnej praxi sa však možno stretnúť s rôznymi skrytými zdravotnými alebo duševnými poruchami zamestnancov, ktorých zdravotným následkom je pocit, že sú takýto zamestnanci stále sledovaní, aj keď to nie je pravda. Rovnako tak sa možno stretnúť s prípadmi

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zneužívania inštitútu sťažnosti, podstatou ktorých je opakované podávania sťažností na porušenie práv zamestnancov, nevynímajúc práva na ochranu súkromia v dôsledku domnelého nezákonného monitorovania, pričom jediným cieľom je administratívna záťaž zamestnávateľa. Takéto podávanie sťažností môže byť výsledkom flustrácie zamestnanca, pocitu ukrivdenia zamestnanca alebo môže byť výsledkom vyhorenia zamestnanca v zamestnaní.

Zákonník práce neupravuje problematiku opakovanej sťažnosti zamestnanca voči zamestnávateľovi alebo inému zamestnancovi v tej istej veci bez doplnenia nových skutočností. Na problematiku šikanózneho výkonu práva zamestnanca voči zamestnávateľovi alebo inému zamestnancovi je potrebné nazerať optikou článku 2 a § 13 ods. 3 Zákonníka práce, podľa ktorého výkon práv a povinností vyplývajúcich z pracovnoprávnych vzťahov musí byť v súlade s dobrými mravmi. Nikto nesmie tieto práva a povinnosti zneužívať na škodu druhého účastníka pracovnoprávneho vzťahu alebo spoluzamestnancov. Výkon práv a povinností v rozpore s dobrými mravmi nepožíva právnu ochranu.

8.3 PRÁVNA OCHRANA PROSTREDNÍCTVOM ZÁSTUPCOV ZAMESTNANCOV

Právna ochrana zamestnanca prostredníctvom zástupcov zamestnancov je realizovaná vo viacerých smeroch. V prvom rade je potrebné upriamiť pozornosť na § 239 Zákonníka práce, na základe ktorého zástupcovia zamestnancov kontrolujú dodržiavanie pracovnoprávnych predpisov vrátane mzdových predpisov a záväzkov vyplývajúcich z kolektívnej zmluvy. Na tento účel sú oprávnení najmä

a) vstupovať na pracoviská zamestnávateľa v čase dohodnutom so zamestnávateľom, a ak sa so zamestnávateľom nedohodnú, najneskôr do troch pracovných dní po oznámení zamestnávateľovi o vstupe na jeho pracoviská,

b) vyžadovať od vedúcich zamestnancov potrebné informácie a podklady,

c) podávať návrhy na zlepšovanie pracovných podmienok,

d) vyžadovať od zamestnávateľa, aby dal pokyn na odstránenie zistených nedostatkov,

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

e) navrhovať zamestnávateľovi alebo inému orgánu poverenému kontrolou dodržiavania pracovnoprávnych predpisov, aby uplatnil vhodné opatrenia voči vedúcim zamestnancom, ktorí porušujú pracovnoprávne predpisy alebo povinnosti vyplývajúce pre nich z kolektívnych zmlúv,

f) vyžadovať od zamestnávateľa informácie o tom, aké opatrenia boli vykonané na odstránenie nedostatkov zistených pri výkone kontroly.

Ak sa zamestnanec domnieva, že jeho právo na ochranu súkromia vyplývajúce z pracovnoprávnych predpisov, z pracovnej zmluvy alebo z kolektívnej zmluvy boli porušené, nemusí konať samostatne, ale môže sa obrátiť na zástupcov zamestnancov. Po oboznámení sa s uvedenou problematikou by mali zástupcovia zamestnancov kontaktovať zamestnávateľa za účelom odstránenia protiprávneho stavu. Právne možnosti zástupcov zamestnancov sú obmedzené na rokovanie so zamestnávateľom, pričom základným právnym nástrojom je kolektívne vyjednávanie v zmysle osobitného predpisu, pričom nie je vylúčené ani právne prostriedky nátlaku voči zamestnávateľovi, ktoré sú upravené v zákone o kolektívnom vyjednávaní. Typickým príkladom je právo na štrajk zamestnancov.

Zákonník práce zveruje zástupcom zamestnancov osobitné právomoci pri ochrane súkromia zamestnancov na pracovisku. Podľa § 13 ods. 4 Zákonníka práce platí, že ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania. Z predmetného ustanovenia Zákonníka práce vyplýva, že pri zavádzaní kontrolného mechanizmu na pracovisku patrí zástupcom zamestnancov právo na prerokovanie tohto mechanizmu v minimálnom rozsahu ohľadom rozsahu kontroly, spôsob jej uskutočnenia, ako aj dobe jej trvania. Súčasne im patrí právo informovať zamestnancov zamestnávateľa o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania. Formu prerokovania týchto náležitostí Zákonník práce nerieši. Možno však pre aplikačnú prax odporučiť, aby sa forma prerokovania uskutočnila v písomnej forme s vyhotovením písomnej zápisnice, kde budú minimálne zachytené náležitosti zavádzania kontrolného mechanizmu na pracovisku zamestnávateľa.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Súčasne úloha zástupcov zamestnancov sa nemusí pri ochrane súkromia zamestnancov na pracovisku obmedzovať len na ustanovenie § 13 ods. 4 Zákonníka práce. Právo zamestnancov na právnu ochranu pri ochrane práva zamestnancov na súkromie sa môže realizovať aj pripomienkovaním alebo návrhom interných normatívnych právnych aktov zamestnávateľa, ktoré rôznym spôsobom upravujú rôzne spôsoby monitorovania zamestnancov na pracovisku zamestnávateľa. V aplikačnej praxi si čoraz viac zamestnávateľov v interných normatívnych právnych aktoch vymedzuje spôsoby a podmienky výkonu monitorovania zamestnancov a kontroly zamestnancov na pracovisku. Súčasťou takýchto interných smerníc veľmi často bývajú zvýšené právomoci zástupcov zamestnancov pri zavádzaní kontrolného mechanizmu alebo pri jeho zmene. Za týmto účelom mávajú zväčša zástupcovia zamestnancov právo na pravidelné kontroly kontrolných mechanizmov zamestnávateľa a účelom preverenia, či nedochádza k nadmerného alebo neoprávnenému zásahu do práva na ochranu súkromia zamestnancov a to napríklad tým, ako sú uschované ich osobné údaje v interných databázach zamestnávateľa.

Súčasne má odborová organizácia zamestnancov právo zastupovať svojich zamestnancov v rámci individuálnych pracovnoprávnych sporov, pri ktorých veľmi často dochádza k neplatnému skončeniu pracovného pomeru so zamestnancami, pričom ako právny podklad neplatného skončenia pracovného pomeru slúži právny záver súdu, že došlo k neoprávnenému zásahu do ochrany súkromia zamestnanca z dôvodu jeho nezákonného sledovania alebo monitorovania.

8.4 PRÁVNA OCHRANA PROSTREDNÍCTVOM ORGÁNOV VEREJNEJ SPRÁVY

Právna ochrana zamestnancov prostredníctvom orgánov verejnej správy a orgánov *sui generis* je reprezentovaná najmä prostredníctvom inšpektorátov práce. Je nutné však zdôrazniť, že v systéme právnej ochrany zamestnanca prostredníctvom orgánov verejnej správy a štátnej správy sa nejedná o jediný spôsob poskytnutia právnej ochrany. Z hľadiska subjektu poskytujúceho právnu ochranu v systéme orgánov verejnej správy a orgánov *sui generis* môžeme zaradiť napríklad:

a) Národný inšpektorát práce a inšpektoráty práce;

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

b) Úrad na ochranu osobných údajov;

c) Úrad na ochranu oznamovateľov protispoločenskej činnosti;

d) Slovenské národné stredisko pre ľudské práva;

e) Verejný ochranca práv.

8.4.1 Národný inšpektorát práce a inšpektoráty práce

Štátnu správu v oblasti inšpekcie práce vykonávajú orgány štátnej správy, ktorými sú Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky, Národný inšpektorát práce a inšpektoráty práce. Národný inšpektorát práce je orgán štátnej správy so sídlom v Košiciach. Národný inšpektorát práce je rozpočtová organizácia. Národný inšpektorát práce riadi a za jeho činnosť zodpovedá generálny riaditeľ Národného inšpektorátu práce. Inšpektoráty práce sú orgány štátnej správy. Inšpektoráty práce sú rozpočtové organizácie. Inšpektorát práce riadi a za jeho činnosť zodpovedá riaditeľ inšpektorátu práce, ktorého na návrh generálneho riaditeľa vymenúva a odvoláva minister práce, sociálnych vecí a rodiny Slovenskej republiky.

Ďalším dôležitým pojmom je inšpekcia práce. **Inšpekcia práce je:**

a) dozor nad dodržiavaním

1. pracovnoprávnych predpisov, ktoré upravujú pracovnoprávne vzťahy, najmä ich vznik, zmenu a skončenie, mzdové podmienky a pracovné podmienky zamestnancov vrátane pracovných podmienok žien, mladistvých, domáckych zamestnancov, osôb so zdravotným postihnutím a osôb, ktoré nedovŕšili 15 rokov veku, a kolektívne vyjednávanie;
2. právnych predpisov, ktoré upravujú štátnozamestnanecké vzťahy;
3. právnych predpisov a ostatných predpisov na zaistenie bezpečnosti a ochrany zdravia pri práci, vrátane predpisov upravujúcich faktory pracovného prostredia;
4. právnych predpisov, ktoré upravujú zákaz nelegálnej práce a nelegálneho zamestnávania;

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

5. záväzkov, ktoré vyplývajú z kolektívnych zmlúv;
6. osobitného predpisu zamestnávateľom v rozsahu jeho povinností uzatvoriť zamestnávateľskú zmluvu a platiť a odvádzať príspevky na doplnkové dôchodkové sporenie za zamestnanca vykonávajúceho práce zaradené orgánom štátnej správy na úseku verejného zdravotníctva do tretej kategórie alebo štvrtej kategórie podľa osobitného predpisu, a za zamestnanca, ktorý vykonáva práce tanečného umelca alebo hudobného umelca, ktorý vykonáva profesiu hráča na dychový nástroj;
7. osobitného predpisu zamestnávateľom, ktorý ustanovuje povinnosti pri vysielaní zamestnancov na výkon prác pri poskytovaní služieb;

b) vyvodzovanie zodpovednosti za porušovanie predpisov uvedených v písmene a) a za porušovanie záväzkov vyplývajúcich z kolektívnych zmlúv;

c) poskytovanie bezplatného poradenstva zamestnávateľom, fyzickým osobám, ktoré sú podnikateľmi a nie sú zamestnávateľmi, a zamestnancom v rozsahu základných odborných informácií a rád o spôsoboch, ako najúčinnejšie dodržiavať predpisy ustanovené v písmene a).

Inšpekcia práce sa vykonáva na všetkých pracoviskách zamestnávateľov a fyzických osôb, ktoré sú podnikateľmi a nie sú zamestnávateľmi, vrátane pracovísk nachádzajúcich sa na súkromných pozemkoch a v obydliach fyzických osôb. Inšpekcia práce sa taktiež vykonáva vo všetkých priestoroch, v ktorých domácky zamestnanec vykonáva dohodnutú prácu a v ktorých zamestnanec vykonáva prácu podľa dohody o prácach vykonávaných mimo pracovného pomeru. Inšpekciu práce vykonáva inšpektor práce. Inšpekcia práce sa **nevykonáva**:

a) na pracoviskách Vojenského spravodajstva, Slovenskej informačnej služby a Národného bezpečnostného úradu,

b) v chránených priestoroch Ministerstva zahraničných vecí Slovenskej republiky,

c) na pracoviskách fyzickej osoby a právnickej osoby, ktoré požívajú diplomatické výsady a imunitu.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Právnym prostriedkom ochrany porušených práv zamestnancov pred príslušným inšpektorátom práce v rámci výkonu inšpekcie práce je **podnet**.

Podľa § 150 ods. 2 Zákonníka práce zamestnanci, ktorí sú poškodení porušením práv alebo povinností vyplývajúcich z pracovnoprávnych vzťahov, ako aj zástupcovia zamestnancov, ktorí sú v pracovnom pomere u zamestnávateľa, u ktorého kontrolnou činnosťou podľa § 239 Zákonníka práce zistili porušenie pracovnoprávnych predpisov, môžu podať podnet na príslušnom orgáne inšpekcie práce. Z uvedeného ustanovenia § 150 ods. 2 Zákonníka práce pre zamestnancov vyplýva, že pokiaľ sú poškodení aj porušením práva na ochranu súkromiav, môžu okrem vyššie spomenutej sťažnosti zamestnávateľovi podať podnet na príslušný orgán inšpekcie práce za účelom jeho preverenia. Na príslušný orgán inšpekcie práce sa rovnako tak v zmysle tohto ustanovenia Zákonníka práce môžu obrátiť aj zástupcovia zamestnancov, ktorí kontrolnou činnosťou v zmysle § 239 Zákonníka práce u zamestnávateľa zistili porušenie pracovnoprávnych predpisov v oblasti porušovania ochrana práva na súkromie zamestnancov. Podľa § 7 ods. 8 písm. c) zákona o inšpekcii práce je inšpektorát práce povinný do 30 dní odo dňa doručenia podnetu vykonať inšpekciu práce. V odôvodnených prípadoch je možné inšpekciu práce vykonať najneskôr do 60 dní od doručenia podnetu. Ak nemožno vzhľadom na povahu veci inšpekciu práce vykonať ani v tejto lehote, môže ju primerane predĺžiť Národný inšpektorát práce. Inšpektorát práce je povinný o predĺžení lehoty, dôvode jej predĺženia a o výsledku inšpekcie práce bezodkladne informovať osobu, ktorá podala podnet.

8.4.2 Úrad na ochranu osobných údajov

V súvislosti s masívnou automatizáciou výrobných procesov, internetizáciou a digitalizáciou práce vystáva čoraz viac do popredia problematika ochrany osobných údajov zamestnancov. V aplikačnej praxi zamestnávateľ spracováva osobné údaje zamestnanca na viaceré účely. V zásade na každé spracovanie osobných údajov zamestnanca musí mať zamestnávateľ právny základ. Osobné údaje zamestnanca určené pre personálnu a mzdovú agendu má zamestnávateľ na základe pracovnej zmluvy, ktorá tvorí právny podklad pre spracovanie osobných údajov zamestnanca. K ďalšiemu spracovaniu osobných údajov môže dôjsť na základe kamerových systémov zamestnávateľa, monitorovania polohy firemných vozidiel zamestnávateľa prostredníctvom GPS systému alebo dronov, prostredníctvom

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

menoviek zamestnancov na ich firemných rovnošatách alebo prostredníctvom fotografií zamestnancov v rôznych informačných a firemných bulletinoch alebo časopisoch.

Pri získavaní súhlasu musí zamestnávateľ dbať na zásady spracovania osobných údajov upravené v § 6 až § 12 zákona o ochrane osobných údajov. Ak prevádzkovateľ žiada o udelenie súhlasu na spracovanie osobných údajov dotknutú osobu, tento súhlas musí byť odlíšený od iných skutočností a musí byť vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme. Ak je spracúvanie osobných údajov založené na súhlase dotknutej osoby, zamestnávateľ je povinný kedykoľvek vedieť preukázať, že zamestnanec poskytol súhlas so spracúvaním svojich osobných údajov. Zamestnanec má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Zakazuje sa spracúvanie osobitných kategórií osobných údajov. Osobitnými kategóriami osobných údajov zamestnanca sú údaje, ktoré odhaľujú jeho rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie zamestnanca.

Medzi osobitné situácie zákonného spracovania osobných údajov zamestnanca podľa § 78 ods. 3 zákona o ochrane osobných údajov patrí situácia, keď prevádzkovateľ, ktorý je zamestnávateľom zamestnanca, je oprávnený poskytovať jeho osobné údaje alebo zverejniť jeho osobné údaje v rozsahu titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresa elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa, ak je to potrebné v súvislosti s plnením pracovných povinností, služobných povinností alebo funkčných povinností zamestnanca. Poskytovanie osobných údajov alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť zamestnanca.

Medzi **práva zamestnanca ako dotknutej osoby** voči prevádzkovateľovi ako zamestnávateľovi **patrí:**

a) právo na prístup k osobným údajom,

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

b) právo na opravu,

c) právo na vymazanie (právo „na zabudnutie“),

d) právo na obmedzenie spracúvania,

e) právo na prenosnosť údajov,

f) právo namietať,

g) právo na to, aby sa na Vás nevzťahovalo automatizované individuálne rozhodovanie vrátane profilovania,

h) právo odvolať súhlas,

i) právo podať návrh na začatie konania o ochrane osobných údajov,

Pokiaľ sa zamestnanec domnieva, že jeho osobné údaje neboli alebo nie sú spracované v súlade so zákonom o ochrane osobných údajov alebo v súlade s Nariadením GDPR, môže si vyššie uvedené práva uplatniť u toho, kto jeho osobné údaje spracováva. Najčastejšie sa jedná práve o zamestnávateľa. Ak má zamestnávateľ ***tzv. zodpovednú osobu***, môže si zamestnanec uplatniť svoje práva u zodpovednej osoby. Žiadosť môže byť ústna, písomná, elektronická prípadne podaná inými prostriedkami. Nariadenie GDPR nepredpisuje konkrétnu formu žiadosti. Odporúča sa využiť najmä písomnú alebo elektronickú formu, aby bolo možné v prípadnom konaní o ochrane osobných údajov preukázať, že ste si svoje právo uplatnili. Zamestnávateľ je povinný vybaviť žiadosť zamestnanca bezodkladne, najneskôr do 1 mesiaca od jej doručenia.

Ak zamestnávateľ v stanovenej lehote neodpovedal alebo žiadosti zamestnanca nevyhovel, zamestnanec sa môže obrátiť na Úrad na ochranu osobných údajov a podať návrh na začatie konania o ochrane osobných údajov podľa zákona o ochrane osobných údajov. Návrh na začatie konania môže zamestnanec podať:

a) písomne v listinnej podobe,

b) písomne v elektronickej podobe autorizovaný podľa osobitného predpisu o elektronickej podobe výkonu verejnej moci; elektronické podanie bez

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

autorizácie podľa osobitného predpisu o elektronickej podobe výkonu verejnej moci (t. j. bežný email bez zaručeného elektronického podpisu) treba do troch pracovných dní doplniť v listinnej podobe, alebo v elektronickej podobe autorizované podľa osobitného predpisu o elektronickej podobe výkonu verejnej moci, alebo osobne na úrade ústnou formou do zápisnice,

c) osobne na úrade ústnou formou do zápisnice.

Návrh na začatie konania musí v zmysle § 100 ods. 3 zákona o ochrane osobných údajov obsahovať:

a) meno, priezvisko, korešpondenčnú adresu a podpis navrhovateľa,

b) označenie toho, proti komu návrh smeruje,

c) predmet návrhu s označením, ktoré práv, ktoré mali byť pri spracúvaní osobných údajov porušené,

d) dôkazy na podporu tvrdení uvedených v návrhu,

e) kópiu listiny alebo iný dôkaz preukazujúci uplatnenie práva podľa druhej časti druhej hlavy zákona o ochrane osobných údajov alebo Nariadenia GDPR, resp. uvedenie dôvodov hodných osobitného zreteľa o neuplatnení predmetného práva.

Ak Úrad na ochranu osobných údajov zistí porušenie práv dotknutej osoby alebo nesplnenie povinností pri spracúvaní osobných údajov, rozhodne predovšetkým o uložení opatrení na nápravu a lehoty na vykonanie nápravného opatrenia. V rozhodnutí môže tiež uložiť pokutu. Ak sa porušenie práv alebo nesplnenie povinností nepreukáže, konanie sa zastaví.

8.4.3 Úrad na ochranu oznamovateľov protispoločenskej činnosti

Protispoločenská činnosť je dynamicky sa rozvíjajúci fenomén, ktorý negatívne ovplyvňuje širokú škálu vzťahov v rámci spoločnosti. Výnimkou v tomto smere nie sú ani právne vzťahy v rámci spoločnosti, v ktorých sa protispoločenská činnosť negatívne prejavuje. Rôzne formy protispoločenskej činnosti môžeme identifikovať aj v rámci pracovnoprávnych vzťahov.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

8.4.3.1 Pojem whistleblowing

Pojem ***whistleblowing*** nie je legislatívnym pojmom a definíciu whistleblowingu nenájdeme v slovenskom právnom poriadku. Pojem whistleblowing pochádza z anglického slovného spojenia *to blow the whistle*, čo v preklade znamená pískať na píšťalku. V kontexte celého ponímania whistleblowingu je možné slovné spojenie *pískanie na píšťalku* chápať ako upozornenie na spoločensky nežiadúci jav.[274] Whistleblowing je možné na účely právnej terminológie v podmienkach slovenskej a českej právnej úpravy preložiť ako oznamovanie, udávanie alebo informovanie.[275] Whistleblowing môže byť v najširšom slova zmysle chápaný ako základné ľudské právo týkajúce sa slobody prejavu, ktorého obsahom je právo slobodne vyjadriť svoj nesúhlas s určitým konaním s cieľom odhaliť protispoločenskú činnosť.

Fenomén whistleblowingu môžeme zaradiť k prierezovým právnym inštitútom, ktoré sa viažu nielen na súkromné právo, ale aj na verejné právo. V oblasti súkromného práva môžeme v rámci tohto pojmu identifikovať rôznorodé pracovnoprávne, občianskoprávne a obchodnoprávne aspekty.[276]

Definovať whistleblowing na účely pracovného práva je možné oznámenie takého konania, ktoré je v rozpore so zákonom, verejným poriadkom, morálkou, politikou alebo stratégiou danej entity a ktoré je v rámci oznamovacích mechanizmov označené ako relevantné a škodlivé.[277] Pojem whistleblowing možno optikou pracovného práva chápať taktiež ako možnosť zamestnanca urobiť oznámenie týkajúce sa nekalých praktík na pracovisku. Oznámenie sa týka nekalých praktík, ktoré ohrozujú ostatných zamestnancov a nie je založené na pocite osobnej krivdy zamestnanca.[278]

---

[274] CÍSAŘOVÁ, E.: Whistleblowing a ochrana oznamovatelů v České republice, Praha: Transparency International, str. 7, ISBN: 978-80-87123-11-9.

[275] MORÁVEK, J.: Několik úvah nad (ne)možnou novelizací Zákoníku práce souvislosti s právní úpravou chráneného oznamování škodlivých jednání, str. 55. In: Acta Universitatis Carolinae – Iuridica 4, 2016, 49 – 71 s., ISSN: ISSN 0323-0619.

[276] PICHRT. J.: Několik poznámek k whistleblowingu, loajalitě zaměstnance a k legislativním návrhům in PICHRT, J. (ed.) Whistleblowing. Praha: Wolters Kluwer ČR, 2013, str. 12 a nasl., ISBN: ISBN 978-80- 7478-393-7.

[277] PICHRT. J., MORÁVEK, J.: Whistleblowing. Právo pro podnikání a zaměstnání, Praha: Comenius Print, č.: 7-8/2009, str. 19, ISSN: 1801-6014.

[278] CALLAND, R., DEHN, G.: Whistleblowing Around the World: Law Culture and Practise, IDASA Publishers, p. 9, ISBN: 978-19-19798-56-1.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

8.4.3.2 Právna úprava whistleblowingu

Základný právny rámec whistleblowingu tvorí Smernica Európskeho parlamentu a Rady 2019/1937 z 23. októbra 2019 o ochrane osôb, ktoré nahlasujú porušenia práva Únie (ďalej len: *„smernica“*).

Slovenská republika prijala dňa 30. januára 2019 vyššie uvedený zákon o ochrane oznamovateľov protispoločenskej činnosti, ktorým sa okrem iného upravili podmienky poskytovania ochrany osobám v pracovnoprávnom vzťahu v súvislosti s oznamovaním kriminality alebo inej protispoločenskej činnosti, pričom protispoločenská činnosť je priamo definovaná v osobitnom právnom predpise. Osobitným právnym predpisom je v tomto prípade zákon č. 583/2008 Z. z. o prevencii kriminality a inej protispoločenskej činnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len: *„zákon o oznamovaní kriminality“*). Podľa § 3 písm. b) a c) zákona o oznamovaní kriminality sa kriminalitou rozumie konanie, ktoré je trestným činom a inou protispoločenskou činnosťou konanie, ktoré je priestupkom alebo iným správnym deliktom. Za inú protispoločenskú činnosť sa považuje aj konanie, ktoré nie je priestupkom alebo iným správnym deliktom, ale pôsobí negatívne na spoločnosť.

8.4.3.3 Protispoločenská činnosť v pracovnoprávnych vzťahoch

Z vyššie uvedenej definície môžeme vyvodiť, že zákon o oznamovaní kriminality nemá uzavretý taxatívny výpočet konaní, ktoré môžeme zaradiť pod protispoločenskú činnosť. Protispoločenskou činnosťou predmetný zákon nerozumie len konanie, ktoré je v osobitných právnych predpisoch výslovne uvedené ako priestupok alebo iný správny delikt, ale aj akékoľvek konanie, ktoré naopak priestupkom alebo iným správnym deliktom nie je, ale pôsobí negatívne na spoločnosť. V tejto súvislosti je preto potrebné vymedziť, ktoré konanie v rámci pracovnoprávnych vzťahov by sme mohli pod definíciu inej protispoločenskej činnosti zaradiť. Táto skutočnosť má v rámci pracovnoprávnych vzťahoch enormný význam, pretože len takému oznamovateľovi protispoločenskej činnosti bude v zmysle zákona o ochrane oznamovateľov protispoločenskej činnosti poskytnutá právna ochrana, ktorý nahlási konanie

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

subjektu, ktoré bude spĺňať v zmysle v § 3 ods. 1 písm. b) a c) zákona o oznamovaní kriminality definíciu kriminality alebo inej protispoločenskej činnosti.

S identifikáciou inej protispoločenskej činnosti, ktorá nie je ako konanie uvedené v osobitných právnych predpisoch ako priestupok alebo iný správny delikt, ale súčasne pôsobí negatívne na spoločnosť, môžu byť v aplikačnej praxi spojené nemalé problémy. Pri identifikácii takejto inej protispoločenskej činnosti nie je totiž priamo rozhodujúce, či takáto iná protispoločenská činnosť má negatívny vplyv na oznamovateľa protispoločenskej činnosti, ale priamo na spoločnosť ako takú. Zväčša pôjde o také konania, ktoré pôsobia negatívne nie len na oznamovateľa protispoločenskej činnosti, ale i na spoločnosť alebo konkrétnu skupinu ľudí (*napríklad kolektív zamestnancov bez ohľadu na konkrétneho zamestnávateľa a zamestnanca*). V pracovnoprávnych vzťahoch pôjde najmä o konanie zamestnávateľa alebo zamestnanca, ktoré bez právneho dôvodu zasahuje do práv alebo právom chránených záujmov iného zamestnanca, resp. celého kolektívnu zamestnancov.

V rámci aplikačnej praxi môžeme identifikovať v pracovnoprávnych vzťahoch niekoľko foriem protispoločenskej činnosti. Môže sa jednať napríklad o:

d) diskrimináciu zamestnancov na pracovisku;

e) rôzne formy obťažovania na pracovisku;

f) mobbing a bossing zo strany zamestnávateľa;

g) šikana zamestnancov na pracovisku;

h) neoprávnené monitorovanie zamestnancov na pracovisku.

8.4.3.4 Pozastavenie účinnosti právneho úkonu

Podľa § 12 ods. 1 zákona o ochrane oznamovateľov protispoločenskej činnosti platí, že ak sa oznamovateľ domnieva, že v súvislosti s oznámením bol voči nemu urobený pracovnoprávny úkon, s ktorým nesúhlasí, môže požiadať úrad do 15 dní odo dňa, keď sa dozvedel o pracovnoprávnom úkone, o pozastavenie účinnosti tohto pracovnoprávneho úkonu.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Za pracovnoprávny úkon možno v zmysle § 7 ods. 1 tohto zákona rozumieť právny úkon alebo vydanie rozhodnutia v pracovnoprávnom vzťahu. Dôležité je, že sa musí jednať o právny úkon zamestnávateľa. Otázkou v tomto smere zostáva konanie zamestnávateľa, ktoré nespĺňa pojmové znaky právneho úkonu v zmysle § 34 Občianskeho zákonníka, ako napríklad pokyn na ***neoprávnené monitorovanie zamestnancov***. Druhou skutočnosťou je, že sa musí jednať o právny úkon alebo rozhodnutie zamestnávateľa. V tomto smere považujeme za relatívne bezproblémové konanie tretích osôb v mene zamestnávateľa, ktorých konanie zamestnávateľa zaväzuje a možno takéto konanie pričítať zamestnávateľovi, avšak predmetný zákon nám nedáva jednoznačnú odpoveď na otázku, či za právny úkon zamestnávateľa možno považovať aj konanie jeho vedúcich zamestnancov alebo akékoľvek iné konanie zamestnávateľa, ktoré z rôznych dôvodov, napríklad excesu z poverenia, nebude zamestnávateľa právne zaväzovať.[279]

Legislatívna formulácia ustanovenia § 12 ods. 1 zákona o ochrane oznamovateľov protispoločenskej činnosti umožňuje zamestnancovi ako oznamovateľovi žiadať o pozastavenie účinnosti pracovnoprávneho úkonu, s ktorým nesúhlasí. Nie je rozhodujúce, či takýto pracovnoprávny úkon je alebo nie je v prospech zamestnanca, aj keď vo väčšine prípadov pôjde o pracovnoprávny úkon s negatívnym dosahom na zamestnanca v postavení oznamovateľa.

Zamestnanec môže požiadať o pozastavenie účinnosti pracovnoprávneho úkonu v lehote 15 dní, z ktorej jednoznačne nevyplýva, o aký typ lehoty sa jedná. V aplikačnej praxi sa môže jednať o hmotnoprávnu prekluzívnu lehotu naviazanú na zánik práva alebo o procesnoprávnu lehotu s tým, že postačuje, aby sa uvedený právny úkon v posledný deň lehoty poslal na poštovú prepravu. Vo všeobecnosti možno povedať, že zákon o ochrane oznamovateľov protispoločenskej činnosti zväčša obsahuje hmotnoprávne normy, avšak s prvkami procesnoprávnych noriem. Pre hmotnoprávnu lehotu svedčí argument, že pri tejto lehote nie je jej zachovanie naviazané na odovzdanie písomnosti na poštovú prepravu, otázkou však je, či sa súčasne jedná o hmotnoprávnu prekluzívnu lehotu, uplynutím ktorej právo zanikne. Sme toho názoru, že aj keď zákon síce za pomoci formulácie *„inak právo zanikne“* neviaže jej

[279] ADAMIČKA, M., DIVÉKYOVÁ, K., POBIJAK, T.: *Konanie podnikateľa.* Praha: Wolters Kluwer ČR, 2020, 120 s.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

uplynutie na zánik práva oznamovateľa protispoločenskej činnosti, jej uplynutím sa oznamovateľ protispoločenskej činnosti nebude môcť domáhať pozastavenia účinnosti konkrétneho pracovnoprávneho úkonu. V opačnom prípade by sme mohli dospieť k situácii, ktorá podľa nášho názoru narušuje stav právnej istoty medzi zamestnávateľom a zamestnancom a uvedená lehota 15 dní by vo svojej podstate stratila opodstatnenie. O povahe tejto lehoty sa bližšie nezmieňuje ani dostupná literatúra.[280]

Účelom samotného pracovnoprávneho inštitútu je pozastavenie účinnosti pracovnoprávneho úkonu. Účinnosť právneho úkonu je jeho vlastnosť, ktorá spôsobuje medzi zmluvnými stranami právne účinky. Od účinnosti zmluvy treba odlíšiť účinky zmluvy. Účinkami zmluvy treba rozumieť dosiahnutie právnych následkov – dôsledkov zmluvy, ktoré sa ňou sledovali.[281] Podľa § 12 ods. 1 zákona o ochrane oznamovateľov protispoločenskej činnosti platí, že oznamovateľ môže požiadať Úrad na ochranu oznamovateľov protispoločenskej činnosti o pozastavenie účinnosti právneho úkonu. Pozastavenie účinnosti je možné len pri platnom právnom úkone. Otázkou v tomto smere je, či je možné žiadať o pozastavenie účinnosti právneho úkonu aj spätne po tom, čo nastali jeho účinky v aplikačnej praxi, ako napríklad pri okamžitom skončení pracovného pomeru. Podľa nášho názoru spätné navrátenie účinkov v aplikačnej praxi pri okamžitom skončení pracovného pomeru nie je možné dosiahnuť podaním žiadosti o pozastavenie účinnosti právneho úkonu v zmysle § 12 ods. 1 zákona o ochrane oznamovateľov protispoločenskej činnosti, ale výlučne len podaním žaloby podľa § 77 a nasl. Zákonníka práce.

8.4.3.5 Súhlas s pracovnoprávny úkonom

Podľa § 7 ods. 1 zákona o ochrane oznamovateľov protispoločenskej činnosti platí, že zamestnávateľ môže urobiť právny úkon alebo vydať rozhodnutie v pracovnoprávnom vzťahu *(t.j. pracovnoprávny úkon)* voči chránenému oznamovateľovi, na ktorý nedal súhlas, len **so súhlasom Úradu na ochranu oznamovateľov protispoločenskej činnosti**. Súhlas Úradu na

[280] MIČUDOVÁ, T. *Zákon o oznamovaní protispoločenskej činnosti. Komentár.* 1. vyd. Bratislava: Wolters Kluwer, 2016, s. 45–47.
[281] BAJÁNKOVÁ, J., VOJČÍK, P. Neplatnosť právnych úkonov a rozhodovacia prax súdov. In: *Ingerencia súdov do súkromnoprávnych zmlúv: Zásahy súdov do obsahu súkromnoprávnych zmlúv.* Pezinok: Justičná akadémia Slovenskej republiky, 2014, s. 20.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ochranu oznamovateľov protispoločenskej činnosti sa nevyžaduje, ak sa pracovnoprávnym úkonom priznáva nárok alebo ak ide o pracovnoprávny úkon súvisiaci so skončením pracovnoprávneho vzťahu, ktorý je dôsledkom právnej skutočnosti, ktorá nezávisí od posúdenia zamestnávateľa. Uvedené ustanovenie zákona príkladom v odkaze uvádza, ktoré ustanovenia Zákonníka práce možno považovať za tie, ktoré predstavujú právnu skutočnosť, ktorá nezávisí od posúdenia zamestnávateľa. Jedná sa napríklad o povinnosť zamestnávateľa preradiť zamestnanca na inú prácu podľa § 55 ods. 2 Zákonníka práce alebo situáciu, kedy podľa § 68 ods. 1 písm. a) Zákonníka práce môže dať zamestnávateľ zamestnancovi okamžité skončenie pracovného pomeru, ak bol právoplatne odsúdený za úmyselný trestný čin.

Ochranu oznamovateľa závažnej protispoločenskej činnosti v podobe udelenia súhlasu s pracovnoprávnym úkonom zákon o ochrane oznamovateľov protispoločenskej činnosti neposkytuje každému oznamovateľovi. Zákon o ochrane oznamovateľov protispoločenskej činnosti poskytuje takúto pracovnoprávnu ochranu len takému oznamovateľovi, ktorý oznámil závažnú protispoločenskú činnosť. Závažnou protispoločenskou činnosťou sa v zmysle § 2 písm. d) bodu 1 až 4 predmetného zákona napríklad rozumie trestný čin, za ktorý Trestný zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou tri roky.[282] Ak z príslušného oznámenia whistleblowera prokurátor alebo správny orgán zistí, že urobil kvalifikované oznámenie, bezodkladne mu poskytne ochranu podľa § 7 tohto zákona a túto skutočnosť oznámi oznamovateľovi, zamestnávateľovi a Úradu na ochranu oznamovateľov protispoločenskej činnosti.[283]

---

282 *„Na účely tohto zákona sa rozumie závažnou protispoločenskou činnosťou:*
1. trestný čin poškodzovania finančných záujmov Európskej únie podľa § 261 až 263 Trestného zákona, trestný čin machinácií pri verejnom obstarávaní a verejnej dražbe podľa § 266 až 268 Trestného zákona, trestné činy verejných činiteľov podľa § 326 až 327a Trestného zákona alebo trestné činy korupcie podľa § 328 až 336b Trestného zákona,
2. trestný čin, za ktorý Trestný zákon ustanovuje trest odňatia slobody s hornou hranicou trestnej sadzby prevyšujúcou tri roky,
3. správny delikt, za ktorý možno uložiť pokutu s hornou hranicou určenou výpočtom, alebo
4. správny delikt, za ktorý možno uložiť pokutu s hornou hranicou vo výške najmenej 30 000 eur.“

283 PORUBAN, A. Vybrané pracovnoprávne aspekty ochrany oznamovateľov na Slovensku, s. 27. In: PICHRT, J., MORÁVEK, J. (eds.) *Whistleblowing – minulost, přítomnost, budoucnost.* Praha: Wolters Kluwer ČR, 2020, 140 s.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Pokiaľ súhlas s pracovnoprávnym úkonom nedá sám chránený oznamovateľ, musí sa zamestnávateľ so svojou žiadosťou obrátiť na Úrad na ochranu oznamovateľov protispoločenskej činnosti. Úrad na ochranu oznamovateľov protispoločenskej činnosti pred vydaním rozhodnutia o žiadosti o udelenie súhlasu umožní chránenému oznamovateľovi vyjadriť sa v primeranej lehote k navrhovanému pracovnoprávnemu úkonu. V jednoduchých veciach, najmä ak možno rozhodnúť len na základe žiadosti zamestnávateľa a vyjadrenia chráneného oznamovateľa, úrad rozhodne o žiadosti o udelenie súhlasu bezodkladne. V ostatných veciach rozhodne úrad do 30 dní odo dňa doručenia žiadosti o udelenie súhlasu. Úrad udelí súhlas s navrhovaným pracovnoprávnym úkonom zamestnávateľa voči chránenému oznamovateľovi, len ak zamestnávateľ preukáže, že navrhovaný pracovnoprávny úkon nemá žiadnu príčinnú súvislosť s kvalifikovaným oznámením, inak žiadosť o udelenie súhlasu zamietne. Proti rozhodnutiu úradu o žiadosti o udelenie súhlasu nemožno podať odvolanie. Od podania žiadosti zamestnávateľa o udelenie súhlasu úradu do právoplatného rozhodnutia o žiadosti o udelenie súhlasu zamestnávateľovi lehoty a skúšobné doby podľa osobitných predpisov neplynú.

Právny úkon, na ktorý úrad neudelil súhlas, je neplatný. Otázkou v tomto smere ostáva, o akú neplatnosť právneho úkonu sa jedná. Podľa nášho názoru sa jedná o absolútnu neplatnosť právneho úkonu, ktorá je svojím obsahom odlišná od neplatnosti právneho úkonu smerujúceho k ukončeniu pracovného pomeru. V zákone o ochrane oznamovateľ jednoznačne absentuje prepojenie na § 77 Zákonníka práce v situácií, kedy zamestnávateľ udelí zamestnancovi výpoveď alebo mu doručí iný právny úkon s negatívnymi právnymi účinkami, na ktorý zamestnávateľ nemal vopred udelený súhlas zo strany Úradu na ochranu oznamovateľov protispoločenskej činnosť. Pri absencii súhlasu s pracovnoprávnym úkonom zamestnávateľa ostáva nezodpovedaná otázka, aký typ žaloby a s akým žalobným návrhom bude musieť podať oznamovateľ závažnej protispoločenskej činnosti voči výpovedi zamestnávateľa, na ktorý nebol vopred udelený súhlas.

8.4.4 Slovenské národné stredisko pre ľudské práva

Medzi ďalšiu inštitúciu, ktorá môže zamestnancom v pracovnoprávnom vzťahu poskytnúť právnu ochranu, je Slovenské národné stredisko pre ľudské práva (ďalej len:

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

„SNSĽP“). Právnym základom pre zriadenie Slovenského národného strediska pre ľudské práva bol zákon č. 308/1993 Z. z. zákon o zriadení Slovenského národného strediska pre ľudské práva v aktuálnom znení (ďalej len: *„zákon o zriadení SNSĽP“*). SNSĽP je nezávislou právnickou osobou. SNSĽP plní úlohy v oblasti ľudských práv a základných slobôd.

Stredisko je oprávnené zastupovať účastníka v konaní vo veciach súvisiacich s porušením zásady rovnakého zaobchádzania podľa antidiskriminačného zákona. SNSĽP za účelom napĺňania svojho cieľa:

a) monitoruje a hodnotí dodržiavanie ľudských práv a dodržiavanie zásady rovnakého zaobchádzania podľa osobitného zákon;

b) zhromažďuje a na požiadanie poskytuje informácie o rasizme, xenofóbii a

c) antisemitizme v Slovenskej republike;

d) uskutočňuje výskumy a prieskumy na poskytovanie údajov v oblasti ľudských práv, zhromažďuje a šíri informácie v tejto oblasti;

e) pripravuje vzdelávacie aktivity a podieľa sa na informačných kampaniach s cieľom zvyšovania tolerancie spoločnosti;

f) zabezpečuje právnu pomoc obetiam diskriminácie a prejavov intolerancie

g) vydáva na požiadanie fyzických osôb alebo právnických osôb alebo z vlastnej iniciatívy odborné stanoviská vo veciach dodržiavania zásady rovnakého zaobchádzania podľa osobitného predpisu;

h) vykonáva nezávislé zisťovania týkajúce sa diskriminácie;

i) vypracúva a uverejňuje nezávislé správy a odporúčania o otázkach súvisiacich s diskrimináciou;

j) poskytuje knižničné služby a

k) poskytuje služby v oblasti ľudských práv.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Z uvedeného dôvodu pokiaľ sa nejaký zamestnanec cíti byť diskriminovaný na svojich právach a právom chránených záujmoch, môže sa so svojím problémom obrátiť na SNSĽP, ktoré daný skutkový prípad právne posúdi a odporučí zamestnancovi ďalší právny postup. Za zamestnanca môže podať na príslušný súd žalobu a zastupovať zamestnanca v konaní pred súdom v rámci individuálnych pracovnoprávnych sporov.

8.4.5 Verejný ochranca práv

Právnym základom pre poskytnutie ochrany zamestnancov prostredníctvom verejného ochrancu práv je zákon č. 564/2001 Z. z. zákon o verejnom ochrancovi práv v aktuálnom znení (ďalej len: *„zákon o VOP“*). Podľa tohto zákona je upravený rozsah a spôsob, ktorým sa verejný ochranca práv ako nezávislý orgán podieľa na ochrane základných práv a slobôd fyzických osôb a právnických osôb pri konaní, rozhodovaní alebo nečinnosti orgánov verejnej moci, ak je ich konanie, rozhodovanie alebo nečinnosť v rozpore s právnym poriadkom alebo princípmi demokratického a právneho štátu.

Podľa § 11 ods. 1 a ods. 2 zákona o VOP platí, že na verejného ochrancu práv sa môže obrátiť každý, kto sa domnieva, že pri konaní, rozhodovaní alebo nečinnosti orgánu verejnej moci boli porušené základné práva a slobody v rozpore s právnym poriadkom alebo princípmi demokratického a právneho štátu. Fyzické osoby môžu v styku s verejným ochrancom práv používať svoj materinský jazyk. Trovy tlmočného znáša štát. Verejný ochranca práv koná na základe podnetu fyzickej osoby alebo právnickej osoby alebo z vlastnej iniciatívy.

Podnet možno podať písomne, ústne do zápisnice, telegraficky, telefaxom alebo elektronickou poštou. Z podnetu musí byť zrejmé, akej veci sa týka, proti ktorému orgánu verejnej moci smeruje a čoho sa podávateľ podnetu domáha. Ak podnet nemá predpísané náležitosti, verejný ochranca práv bezodkladne vyzve podávateľa podnetu, aby v určenej lehote, ktorá nesmie byť kratšia ako sedem dní, neúplný alebo nejasný podnet doplnil alebo spresnil. Poučí ho aj o tom, ako treba doplnenie alebo spresnenie urobiť.

Ak výsledkami vybavenia podnetu nie je preukázané porušenie základných práv a slobôd, verejný ochranca práv písomne o tom upovedomí podávateľa podnetu a orgán verejnej moci, proti ktorého postupu, rozhodovaniu alebo nečinnosti podnet smeruje. Ak výsledkami

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

vybavenia podnetu je preukázané porušenie základných práv a slobôd, verejný ochranca práv oznámi výsledky vybavenia podnetu spolu s návrhom opatrení orgánu verejnej moci, proti ktorého postupu, rozhodovaniu alebo nečinnosti podnet smeruje. Ak pri vybavovaní podnetu verejný ochranca práv zistí skutočnosti nasvedčujúce tomu, že pri činnosti orgánu verejnej moci bol spáchaný trestný čin, priestupok, iný správny delikt alebo disciplinárne previnenie alebo že bola porušená povinnosť ustanovená zákonom, oznámi to príslušnému orgánu.

Ak pri vybavovaní podnetu verejný ochranca práv zistí skutočnosti nasvedčujúce tomu, že zákon, iný všeobecne záväzný právny predpis alebo vnútorný predpis vydaný orgánom verejnej moci porušuje základné práva a slobody fyzických osôb a právnických osôb, môže podať podnet na jeho zmenu alebo zrušenie príslušnému orgánu. Verejný ochranca práv písomne upovedomí o výsledkoch vybavenia podnetu a o prijatých opatreniach podávateľa podnetu a osobu, ktorej základné práva a slobody boli konaním, rozhodovaním alebo nečinnosťou orgánov verejnej moci porušené.

V aplikačnej praxi sa na verejného ochrancu práv môže obrátiť zamestnanec, ktorého podnet na inšpektorát práce alebo na Úrad na ochranu osobných údajov týkajúci sa porušovania práva na súkromie zamestnanca na pracovisku alebo z dôvodu ochrany práva na ochranu svojich osobných údajov nebol vôbec vyriešený alebo nebol vyriešený v stanovenej lehote, prípadne pre jeho nezákonnosť došlo k porušeniu práva zamestnanca. Pôsobnosť verejného ochrancu práv sa síce nevzťahuje na rozhodovaciu činnosť všeobecných súdov, vzťahuje sa však na orgány riadenia a správy súdov, čo v aplikačnej praxi znamená, či v konkrétnom pracovnoprávnom spore medzi zamestnávateľom a zamestnancom nedochádza k porušovaniu práva na spravodlivý proces bez neprimerane dlhých prieťahov nečinnosťou súdu.

8.4.6 Právna ochrana prostredníctvom mediátora

Riešenie pracovnoprávnych sporov prostredníctvom mediácie patrí k alternatívnym spôsobom riešenia pracovnoprávnych sporov medzi zamestnávateľom a zamestnancom. Právnym základom na riešenie pracovnoprávnych sporov prostredníctvom mediácie je zákon č. 420/2004 Z. z. zákon o mediácii v znení neskorších predpisov (ďalej len: *„zákon o mediácii“*)

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

. Podľa § 2 ods. 1 zákona o mediácii je mimosúdna činnosť, pri ktorej osoby zúčastnené na mediácii pomocou mediátora riešia spor, ktorý vznikol z ich zmluvného vzťahu alebo iného právneho vzťahu. Podľa § 1 ods. 2 zákona o mediácii platí, že tento zákon sa vzťahuje na spory, ktoré vznikajú z občianskoprávnych vzťahov, rodinnoprávnych vzťahov, obchodných záväzkových vzťahov a pracovnoprávnych vzťahov. Z uvedeného dôvodu je možné spory medzi zamestnávateľom a zamestnancom riešiť aj prostredníctvom mediácie pred mediátorom. Mediátorom podľa tohto zákona môže byť každá fyzická osoba zapísaná v registri mediátorov, na ktorej sa osoby zúčastnené na mediácii dohodnú a ktorá s osobami zúčastnenými na mediácii uzavrie dohodu o začatí mediácie podľa § 14 ods. 1 zákona o mediácii. Výkon činnosti mediátora je podnikaním.

Ustanovenie § 14 ods. 1 zákona o mediácii upravuje začiatok konania. V dohode o začatí mediácie sa osoby zúčastnené na mediácií s mediátorom dohodnú na mediácii konkrétneho sporu; dohoda musí mať písomnú formu a označuje sa poradovým číslom podľa evidencie vedenej mediátorom v knihe mediácií. Dohoda o začatí mediácie obsahuje najmä

a) presné označenie osôb zúčastnených na mediácii;

b) presné označenie mediátora a jeho kancelárie;

c) vymedzenie konkrétneho sporu, ktorý je predmetom mediácie;

d) výšku odmeny mediátora, spôsob jej určenia alebo dohodu o bezplatnom výkone mediácie a

e) dobu, na ktorú je uzavretá, alebo dobu, počas ktorej má mediácia prebiehať.

V prípade úspešného skončenia pracovnoprávneho sporu pred mediátorom sa konanie končí v zmysle § 14 ods. 8 písm. a) zákona o mediácii dňom uzavretia dohody, ktorá je výsledkom mediácie. Účinky takejto dohody o mediácii sú upravené v § 15 zákona o mediácii. Podľa § 15 ods. 1 zákona o mediácii dohoda, ktorá vznikla ako výsledok mediácie, má písomnú formu a je pre osoby zúčastnené na mediácii záväzná. Na základe dohody, ktorá vznikla ako výsledok mediácie, môže oprávnený podať návrh na súdny výkon rozhodnutia alebo návrh na

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

vykonanie exekúcie, ak je táto dohoda podľa podmienok ustanovených v osobitných predpisoch spísaná vo forme notárskej zápisnice alebo schválená ako zmier pred súdom.

Na základe vyššie uvedených účinkov dohody o mediácii možno stranám pracovnoprávneho sporu týkajúceho sa napríklad aj porušovania práva na ochranu súkromia zamestnanca na pracovisku odporučiť, aby uvedenú dohodu o mediácii uzatvorili vo forme notárskej zápisnice alebo ako schválený zmier v prípade, ak sa vedie súčasne súdne konanie ohľadne pracovnoprávneho sporu, pretože v opačnom prípade takáto dohoda o mediácii nebude spôsobilým exekučným titulom na jej vykonanie v zmysle Exekučného poriadku. Aj v takomto prípade sú však sporové strany pracovnoprávneho sporu povinné sa správať podľa výsledkov takejto dohody o mediácii, pretože je pre nich právne záväzná.

8.4.7 Právna ochrana prostredníctvom súdu

Podľa článku 9 Zákonníka práce zamestnanci a zamestnávatelia, ktorí sú poškodení porušením povinností vyplývajúcich z pracovnoprávnych vzťahov, môžu svoje práva uplatniť na súde. Zamestnávatelia nesmú znevýhodňovať a poškodzovať zamestnancov preto, že zamestnanci uplatňujú svoje práva vyplývajúce z pracovnoprávnych vzťahov. Podľa § 14 Zákonníka práce platí, že spory medzi zamestnancom a zamestnávateľom o nároky z pracovnoprávnych vzťahov prejednávajú a rozhodujú súdy.

Zákonník práce sa v niektorých svojich ustanoveniach vyslovene zmieňuje o práve zamestnanca obrátiť sa so svojou žalobou na príslušný súd. Konkrétne sa jedná o možnosť zamestnanca obrátiť sa na súd aj v prípade neoprávneného narušenia súkromia zamestnanca podľa § 13 ods. 4 Zákonníka práce. Medzi najčastejšie žaloby na ochranu súkromia môžeme zaradiť:

a) žaloba na upustenie od neoprávneného zásahu (tzv. negatórna žaloba);

b) žaloba na odstránenie následkov takýchto zásahov (tzv. reštitučná žaloba);

c) žaloba na poskytnutie primeraného zadosťučinenia (tzv. satisfakčná žaloba).

Uvedené žaloby sa môžu medzi sebou kumulovať alebo môžu byť uplatnené samostatne. Ich kumulatívne uplatnenie v žalobnom návrhu závisí od typu zásahu do ochrany

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

práva na súkromie zamestnanca a od účelu, ktorý chce zamestnanec prostredníctvom týchto právnych prostriedkov na súde dosiahnuť. Svoje žalobné nároky môže zamestnanec voči zamestnávateľovi uplatniť v rámci individuálneho pracovnoprávneho sporu na súde.

Základom pre individuálne pracovnoprávne spory je Civilný sporový poriadok. Podľa § 316 ods. 1 a ods. 2 Civilného sporového poriadku individuálny pracovnoprávny spor na účely tohto zákona je spor medzi zamestnancom a zamestnávateľom vyplývajúci z pracovnoprávnych a iných obdobných pracovných vzťahov. Za individuálny pracovnoprávny spor sa považuje aj spor, ktorý vyplýva zo zásady rovnakého zaobchádzania, ak súvisí s individuálnym pracovnoprávnym sporom. Individuálne pracovnoprávne spory sú spory s ochranou slabšej strany, ktorou je v tomto prípade zamestnanec. Individuálne pracovnoprávne spory sa pred všeobecnými súdmi vyznačujú určitými špecifikami, ktorými napríklad sú:

a) kauzálna príslušnosť pracovnoprávnych súdov;

b) možnosť zastúpenia zamestnanca odborovou organizáciu;

c) osobitná poučovacia povinnosť súdu oči zamestnancovi;

d) možnosť súdu vykonať dôkazy, ktoré zamestnanec sám nenavrhol;

e) neuplatnenie sudcovskej a zákonnej koncentrácii konania;

f) nemožnosť vydania rozsudku pre zmeškanie v neprospech zamestnanca.

Zamestnanec sa môže dať v individuálnom pracovnoprávnom spore zastupovať odborovou organizáciou. Súd pri prvom procesnom úkone vo vzťahu k zamestnancovi vhodným spôsobom zamestnanca poučí o možnosti zastúpenia a jeho procesných právach a povinnostiach nielen v rozsahu všeobecnej poučovacej povinnosti, ale poučí ho aj o dôkazoch, ktoré je potrebné predložiť, o možnosti podať návrh na neodkladné opatrenie alebo zabezpečovacie opatrenie a o iných možnostiach potrebných na účelné uplatnenie alebo bránenie jeho práv. Súd môže vykonať aj tie dôkazy, ktoré zamestnanec nenavrhol, ak je to nevyhnutné pre rozhodnutie vo veci. Súd aj bez návrhu obstará alebo zabezpečí taký dôkaz; na tento účel je zamestnávateľ povinný poskytnúť súčinnosť, ak to možno od neho spravodlivo

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

žiadať. Zamestnanec môže predložiť alebo označiť všetky skutočnosti a dôkazy na preukázanie svojich tvrdení najneskôr do vyhlásenia rozhodnutia vo veci samej. Ustanovenia o sudcovskej koncentrácii konania a zákonnej koncentrácii konania sa nepoužijú. Ustanovenia o rozsudku pre zmeškanie sa nepoužijú, ak by mal byť tento rozsudok vydaný v neprospech zamestnanca. Súd na prejednanie sporu nariadi pojednávanie. Pojednávanie nie je potrebné nariadiť, ak s tým strany súhlasia a neodporuje to účelu tohto zákona.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

9 OCHRANA SÚKROMIA OSOBITNÝCH KATEGÓRII ZAMESTNANCOV

Právna úprava osobitných kategórii zamestnancov sa zvykne vyznačovať osobitnou právnou úpravou niektorých právnych, resp. pracovnoprávnych inštitútov, ktoré sú legislatívne upravené potrebám aplikačnej praxe pre konkrétnu skupinu zamestnancov. Právna ochrana súkromia osobitných kategórii zamestnancov nie je v tomto smere žiadnou výnimkou. Pre účely našej vedeckej analýzy sme vybrali profesionálnych športovcov, profesionálnych vodičov, a sudcov všeobecných súdov, ktorých môžeme zaradiť medzi osobitné kategórie zamestnancov s akcentom na rozdielnu právnu úpravu ochrany ich súkromia, ktorá vyplýva z osobitných právnych predpisov alebo zo špecifickosti ich výkonu práce.

9.1 OCHRANA SÚKROMIA PROFESIONÁLNYCH ŠPORTOVCOV

Vo všeobecnosti možno povedať, že aj profesionálni športovci bez ohľadu na ich právny status, na základe ktorého vykonávajú svoju profesionálnu športovú činnosť, majú právo na ochranu súkromia. S postupným zavádzaním nových technológií v oblasti športu s masívnou digitalizáciou športového prostredia sa začali objavovať nové formy monitorovania profesionálnych športovcov, ktoré okrem iného zasahujú do práva na ochrany súkromia profesionálnych športovcov. Typickým príkladom je sledovanie príjmu a výdaju kalórií za určité sledovacie obdobie profesionálneho športovca, sledovanie odbehaných kilometrov prostredníctvom monitorovacích zariadení určených pre profesionálnych futbalových rozhodcov v domácom prostredí mimo predsezónnych previerkových seminárov, monitorovacie systémy vyhodnocujúce aktuálne výsledky športovej výkonnosti profesionálneho športovca, alebo napríklad monitorovanie profesionálnych športovcov prostredníctvom dronov počas tréningových jednotiek alebo športových zápasov a podujatí. Zásahy do súkromia profesionálnych športovcov môžu byť spôsobené samotným zamestnávateľom v právnom postavení športovej organizácie alebo treťou osobou, ktorá môže byť zamestnancom zamestnávateľa vo vedúcej pozícií k profesionálnemu športovcovi (hlavný tréner) alebo treťou osobou, akou je napríklad televízia, dopingový komisár alebo zamestnanec národného športového zväzu. Na základe vyššie uvedených kritérií určených na vyhodnotenie oprávnenosti alebo neoprávnenosti zásahu do ochrany súkromia

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

profesionálnych športovcov je potrebné uviesť, že nie všetky spomínané zásahy do ochrany súkromia profesionálnych športovcov budú v oblasti športu vyhodnotené ako neoprávnené a teda uskutočnené v rozpore so zákonom. V tomto prípade bude hrať dôležitú úlohu skutočnosť, že oblasť športu predstavuje špecifické pracovné prostredie, v ktorom profesionálni športovci vykonávajú športovú činnosť. Špecifické športové prostredie profesionálneho športovca v kontexte ochrany jeho súkromia spočíva najmä v tom, že šport ako oblasť hospodárskej činnosti je stredobodom záujmu celej spoločnosti, kde existuje verejný záujem a celospoločenský konsenzus na tom, aby sa športové zápasy vysielali v priamych prenosoch na rôznych televíznych staniciach alebo internetových streamoch. Rovnako tak existuje celospoločenský záujem na tom, aby oblasť športu bola bez dopingu, pričom samotná dopingová kontrola predstavuje určitý typ zásahu do ochrany súkromia profesionálneho športovca, pričom tento zásah do ochrany súkromia práv profesionálneho športovca je odôvodnený verejným záujmom spoločnosti na tom, aby sa profesionálna športová činnosť vykonávala bez dopingu profesionálnych športovcov, čo je následne pretavené do antidopingového kódexu WADA, kde je upravený postup pri výkone dopingovej kontroly u profesionálnych športovcov. Pri vyššie spomenutých zásahov do ochrany súkromia profesionálnych športovcov nielenže nemožno automaticky uzatvoriť, že sa jedná o neoprávnený zásah do ochrany súkromia profesionálnych športovcov, ale niektoré zásahy do ochrany súkromia sú následne spojené s finančnou kompenzáciou v prospech národných športových zväzov, športových organizácií a následne aj profesionálnych športovcov titulom vysielacích a reklamných práv spojených s televíznymi a internetovými prenosmi počas ich športových výkonov.

Osobitnú právnu úpravu ochrany súkromia profesionálnych športovcov upravuje aj slovenský ZoŠ. Podľa § 5 ods. 6 a ods. 7 ZoŠ platí, že : „Pri vykonávaní športu môže byť športovec bez jeho súhlasu monitorovaný športovou organizáciou, ku ktorej má príslušnosť, ak § 90 ods. 3 neustanovuje inak. Z monitorovania môžu byť vyhotovované obrazové, zvukové, obrazovo-zvukové záznamy a záznamy o fyzickej výkonnosti športovca. Záznamy z monitorovania uchováva športová organizácia, ku ktorej má športovec príslušnosť, najviac 12 rokov odo dňa ich vyhotovenia. Monitorovanie športovca podľa odseku 6 je možné iba na

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

účely posudzovania športového výkonu športovca, prípravy športovca alebo majetkového zhodnotenia záznamov športovou organizáciou. Použitie záznamov nesmie byť v rozpore s oprávnenými záujmami športovca a nesmie bezdôvodne zasahovať do jeho práva na ochranu súkromia nad rámec nevyhnutný na dosiahnutie účelu monitorovania a zaznamenávania športového výkonu športovca. Z uvedeného ustanovenia ZoŠ vyplýva, že monitorovanie profesionálneho športovca je možné iba pre účely posudzovania jeho športového výkonu, prípravy športovca alebo majetkového zhodnotenia záznamov športovou organizáciou. Použitie uvedených záznamov nesmie byť použité v rozpore s oprávnenými záujmami profesionálneho športovca. Súčasne použitie takýchto záznamov nesmie bez právneho dôvodu zasahovať do práva na ochranu súkromia profesionálneho športovca nad rámec nevyhnutý na dosiahnutie účelu monitorovania športového výkonu profesionálneho športovca. Súčasne z uvedeného ustanovenia vyplýva, že monitorovanie profesionálneho športovca sa môže uskutočniť bez jeho súhlasu len v prospech športovej organizácie. Akékoľvek iné monitorovanie profesionálneho športovca sa môže uskutočniť len s jeho súhlasom. Takýto súhlas nie je potrebný pre verejnoprávne a súkromnoprávne médiá, pričom akékoľvek ďalšie súhlasy s vyhotovením obrazových, zvukových a zvukovo-obrazových záznamov môže byť predmetom vzájomných mediálnych, marketingových a reklamných práv a povinností, ktoré vyplývajú z ďalších zmluvných vzťahov medzi profesionálnymi športovcami a tretími subjektmi. Aj v tomto prípade platí, že zásah do práva na súkromný život profesionálneho športovca je možný len na základe splnenia troch kritérií, a to kritéria legality, legitimity a proporcionality.

Podľa § 7 ods. 7 ZoŠ platí, že: „pri vykonávaní činnosti športového odborníka môže byť športový odborník bez jeho súhlasu monitorovaný športovou organizáciou, ku ktorej má príslušnosť, a z monitorovania môžu byť vyhotovované obrazové, zvukové alebo obrazovo-zvukové záznamy, ak § 90 ods. 3 neustanovuje inak. Podmienky monitorovania podľa § 5 ods. 6 a 7 sa na športového odborníka vzťahujú rovnako.“ Medzi športových odborníkov môžeme zaradiť napríklad aj rozhodcov daného športu, na ktorých zásady monitorovania profesionálnych športovcov platia rovnako.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Podľa § 48 ods. 4 písm. e) a f) ZoŠ medzi podstatné náležitosti zmluvy o príprave talentovaného športovca patrí záväzok športovej organizácie monitorovať individuálne športové zručnosti a schopnosti talentovaného športovca a súčasne záväzok zostaviť individuálny plán prípravy zameraný na rozvoj športových zručností a schopností talentovaného športovca v nadväznosti na monitorovanie podľa písmena e). Z uvedeného ustanovenia ZoŠ dokonca vyplýva zákonná a následne aj zmluvná povinnosť športovej organizácie (športového klubu) monitorovať profesionálneho športovca. ZoŠ bližšie nešpecifikuje prostriedky, akými má športová organizácia povinnosť profesionálneho talentovaného športovca monitorovať. Sme toho názoru, že zvolené monitorovacie prostriedky a technika monitorovania musia byť primerané okolnostiam a účely, na aký sa profesionálny športovec monitoruje. V zásade platí, že menej invazívne prostriedky monitorovania profesionálneho športovca majú prednosť pred invazívnymi prostriedkami monitorovania profesionálneho talentovaného športovca na základe zásady proporcionality.

Podľa § 90 ods. 3 ZoŠ upravuje na národnej úrovni postup pri výkone dopingovej kontroly, podľa ktorého: „v priestoroch výkonu dopingovej kontroly, ktoré boli na tento účel poskytnuté organizátorom súťaže, sa nesmú vyhotovovať žiadne obrazové záznamy, zvukové záznamy alebo zvukovo-obrazové záznamy.“ Legislatívny zákaz vyhotovovania uvedených záznamov súvisí s ochranou súkromia profesionálnych športovcov pri odbere biologických materiálov pri dopingovej kontrole. Najmä pri dopingových kontrolách je potrebné dbať na potrebu zvýšenej ochrany súkromia profesionálnych športovcov. Na jednej strane platí zákaz pre akékoľvek osoby prítomné pri dopingovej kontrole vyhotovovať obrazové záznamy, zvukové záznamy alebo zvukovo-obrazové záznamy, no na druhej strane sú dopingové miestnosti vybavené pri sociálnych zariadeniach umiestnenými zrkadlami v stanovenej výške, aby mal dopingový komisár rovnakého pohlavia ako profesionálny športovec dobrú viditeľnosť na odoberaný biologický materiál profesionálneho športovca tak, aby nedochádzalo pri jeho odbere k zámene alebo k znehodnoteniu biologického materiálu, pričom logicky dochádza k zvýšenému tlaku na ochranu práva na súkromie profesionálneho športovca, ktorý takýto postup musí strpieť.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Zákon č. 1/2014 Z.z. zákon o organizácii verejných športových podujatí v znení neskorších predpisov (ďalej len: *„zákon“*) upravuje podmienky konania verejných športových podujatí. Tento zákon upravuje aj podmienky výkon delegáta zväzu, ktorý priamo na športovom podujatí vykonáva dohľad nad dodržiavaním tohto zákona ako aj interných normatívnych právnych aktov národných športových zväzov. Podľa § 19 ods. 5 zákona platí, že: *„delegát zväzu je oprávnený v súvislosti s vykonávaním dozoru na podujatí vyhotovovať obrazové, zvukové alebo iné záznamy preukazujúce nevhodné konanie alebo správanie účastníkov podujatia a plnenie povinností organizátora podujatia vrátane zistených nedostatkov a opatrení prijatých na ich odstránenie.“* Na základe tohto ustanovenia môže delegát zväzu vyhotovovať akékoľvek obrazové, zvukové alebo iné záznamy súvisiace s porušovaním tohto zákona na športových podujatiach a zaslať ich spolu so správou delegáta národného športovému zväzu. Nezriedka sú predmetom takýchto videozáznamov aj profesionálni športovci, ktorí sa rôznym spôsobom môžu previniť proti iným profesionálnych športovcov alebo divákom na športovom podujatí, pričom delegát zväzu v právnom postavení zamestnanca národného športového zväzu je v zmysle tohto zákonného ustanovenia oprávnený vyhotoviť uvedené záznamy osvedčujúce priebeh udalostí na tomto športovom podujatí a zaslať ich so správou delegáta národnému športovému zväzu. Delegát zväzu ich však nesmie zneužiť na súkromné účely a predmetné ustanovenie naráža na aplikačné problémy súvisiace so spracovaním a uchovávaním osobných údajov iných profesionálnych športovcov na súkromných mobilných zariadeniach delegátov zväzu podľa osobitného predpisu, ktorým je zákon o ochrane osobných údajov a príslušné nariadenie GDPR.

9.2 OCHRANA SÚKROMIA PROFESIONÁLNYCH VODIČOV

Monitorovanie zamestnancov v cestnej doprave je v súčasnej dobe už pomerne bežnou aplikačnou praxou zamestnávateľov. Aktuálne sú na zamestnancov v cestnej doprave vyvíjané vysoké pracovné nároky, ktoré sú kontrolované a monitorované rôznymi spôsobmi zo strany zamestnávateľov. V tejto časti našej vedeckej analýzy poukážeme na jednotlivé spôsoby kontroly a monitorovania zamestnancov v cestnej doprave, pričom upozorníme na aplikačné nedostatky aktuálnej právnej úpravy, ktorá priamo súvisí s monitoringom zamestnancov v cestnej doprave.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

9.2.1 Spôsoby a dôvody monitorovania zamestnancov v cestnej doprave

Medzi jednotlivé spôsoby monitorovania zamestnancov určite patrí monitorovanie zamestnancov prostredníctvom GPS systému, kontrola zamestnancov na základe vykonania orientačnej dychovej skúšky zo strany zamestnávateľa pred jazdou vodiča, osobná prehliadka vodiča, kontrola výkonu práce prostredníctvom mystery shoppingu, monitorovanie zamestnancov prostredníctvom dronov, monitorovanie zamestnancov prostredníctvom kamerového systému alebo monitorovanie zamestnancov v podobe informatívnych meračov rýchlosti v areáloch výrobných podnikoch zamestnávateľov. V kontexte nami vyššie naznačeného delenia spôsobov monitorovania zamestnancov môžeme konštatovať, že v širokej škále možností, akými spôsobmi možno monitorovať zamestnancov v cestnej doprave, môžeme nájsť klasické spôsoby monitorovania zamestnancov ale aj nové moderné a sofistikované spôsoby monitorovania zamestnancov ako napríklad monitorovanie zamestnancov prostredníctvom GPS systému.

Najčastejším subjektom, ktorý vykonáva kontrolu zamestnancov v cestnej doprave patrí určite sám zamestnávateľ. V kontexte širšieho chápania monitorovania zamestnancov, ktoré sa uskutočňuje za účelom dodržiavania sociálnych práv zamestnancov v cestnej doprave, je subjektom vykonávajúcim kontrolu príslušník Policajného zboru Slovenskej republiky v spolupráci s inšpektorom práce. V kontexte širšieho chápania monitorovania zamestnancov netreba zabúdať na samotných cestujúcich, ktorí prostredníctvom rôznych aplikácií môžu priamo anonymne ohodnotiť výkon práce zamestnancov pracujúcich v doprave. S rozvojom nových technológií v oblasti cestnej dopravy ku kontrolovaným subjektom už dávno nepatria len profesionálni vodiči z povolania, ale sú to napríklad stewardi, ktorí sa starajú o palubný servis cestujúcich v autobusoch. Monitorovanie zamestnancov v cestnej doprave sa môže uskutočniť s vedomím zamestnanca alebo bez jeho vedomia skrytou formou. Pokiaľ zamestnancov hodnotia samotní cestujúci, tak s najväčšou pravdepodobnosťou sa bude jednať o anonymne hodnotenie.

Medzi najčastejšie dôvody zavádzania monitorovacích zariadení v cestnej doprave v intenciách vyššia uvedeného určite patrí finančná optimalizácia dopravných výkonov v osobnej a nákladnej cestnej doprave alebo ochrana vlastníckeho práva zamestnávateľa.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Netreba však zabúdať, že takmer v každom jednom spôsobe monitorovania zamestnancov v cestnej doprave môžeme nájsť prvky zvýšenia bezpečnosti a ochrany zdravia pri práci samotných zamestnancov, ktoré sa následne môžu prejaviť k prispeniu celkovej bezpečnosti všetkých účastníkov cestnej premávky na pozemných komunikáciách.

9.2.2 Monitorovanie GPS systémom

V súčasnej dobe sa medzi zamestnávateľmi vykonávajúcimi dopravné služby najviac rozšírilo monitorovanie zamestnancov prostredníctvom GPS systému (z angl. *„Global Positing System“*), ktorí pri výkone svojej práce využívajú motorové vozidlo. Tento spôsob monitorovania zamestnancov sa stal u väčšiny verejných dopravných prostriedkov ich pravidelnou súčasťou. Podstatou GPS systému je, že umožňuje zamestnávateľovi sledovať a vyhodnocovať pomocou príslušného počítačového programu rýchlosť motorového vozidla, lokalizovať aktuálnu polohu motorového vozidla, pracovný čas a doby odpočinku vodiča motorového vozidla a s tým súvisiace údaje. Pokým z technického hľadiska pri inštalácii a používaní GPS systému v aplikačnej praxi zo strany zamestnávateľov sa nevyskytujú veľké problémy, tak z pohľadu ústavného práva a pracovného práva v kontexte ochrany súkromia zamestnanca predstavuje monitorovanie zamestnancov prostredníctvom GPS systému výrazný aplikačný problém. Pokiaľ sa zamestnávateľ rozhoduje zaviesť do služobného motorového vozidla GPS systém, v prvom rade si musí odpovedať na otázku, či existujú na jeho strane vážne dôvody spočívajúce v jeho činnosti v zmysle § 13 ods. 4 Zákonníka práce, ktoré predstavujú *condicio sine qua non* pre zamestnávateľa, pretože k narušeniu súkromia zamestnanca môže dôjsť len z vážnych dôvodov existujúcich na strane zamestnávateľa. Najčastejšie sa inštalácia GPS systému do motorových vozidiel odôvodňuje ekonomickými dôvodmi na strane zamestnávateľa v kontexte optimalizácie daňových výdavkov alebo ochranou majetku zamestnávateľa pred odcudzením alebo poškodeným. Ďalším legitímnym účelom inštalácie GPS systému do motorových vozidiel je zvýšenie BOZP a eliminácia dopravných nehôd v kontexte vzniku pracovných úrazov samotných zamestnancov pracujúcich u zamestnávateľa.[284] Vo všeobecnosti je možné predpokladať, že takéto vážne

[284] SISKOVIČOVÁ, K.: Ochrana súkromia zamestnanca a ochrana súkromia zamestnanca, 1. vyd., Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, 149 s., ISBN: 978-80-8082-932-2.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

dôvody na strane zamestnávateľa by mali byť naplnené v prípadoch, keď zamestnávatelia poskytujú svoje služby v rámci sektora verejnej dopravy alebo ktorí využívajú pri poskytovaní svojich tovarov a služieb osobnú alebo nákladnú cestnú dopravu alebo prepravu z vyššie uvedených dôvodov. V druhom rade je potrebné zodpovedať otázku, či narušenie súkromia zamestnanca prostredníctvom GPS systému sa uskutočňuje na pracovisku zamestnávateľa alebo v spoločných priestoroch zamestnávateľa. Zákonník práce pojem pracovisko nevymedzuje. Za pracovisko treba podľa odbornej literatúry považovať určitý priestor, v ktorom má zamestnanec vykonávať svoju prácu. Môže ním byť napríklad príslušná kancelária, dielňa, stavenisko.[285] Podľa rozhodnutia Najvyššieho súdu Českej republiky: *„pracoviskom sa rozumie miesto, kde zamestnanec plní podľa pokynov zamestnávateľa svoje pracovné úlohy.“*[286] Podľa § 8 ods. 4 pís. d) zákona č. 462/2007 o organizácii pracovného času v doprave v znení neskorších predpisov (ďalej len: *„zákon o organizácii pracovného času v doprave“*) sa pracoviskom mobilného zamestnanca v doprave rozumie aj dopravný prostriedok, ktorý mobilný zamestnanec využíva na vykonávanie dopravných činností. V aplikačnej praxi sa v monitorovanom vozidle prostredníctvom GPS systému vyskytujú aj iní zamestnanci, ktorí sa svojou činnosťou podieľajú na zabezpečení bezpečnosti a plynulosti osobného dopravného prostriedku alebo bezproblémovom poskytovaní služieb na palube osobného dopravného prostriedku. Najčastejšie sa jedná o vodičov sediacich na sedadle spolujazdca alebo stewardov v autobusoch, ktorí poskytujú cestujúcim služby palubného personálu. Z uvedeného dôvodu je potrebné skúmať, kto sa v aplikačnej praxi považuje za mobilného zamestnanca v cestnej doprave. Podľa § 7 ods. 1 zákona o organizácii pracovného času v doprave platí, že za mobilných zamestnancov v cestnej doprave sa považujú vodiči a ďalší členovia cestujúceho personálu, ktorí vykonávajú dopravné činnosti v cestnej doprave pre zamestnávateľa v pracovnom pomere. Z vedenej definície mobilných zamestnancov nám vzniká prvý aplikačný problém súvisiaci s výkonom práce profesionálneho vodiča na základe jednej z dohôd o vykonaní práce mimo pracovného pomeru, nakoľko takýto vodiči nevykonávajú závislú prácu v pracovnom pomere u zamestnávateľa v zmysle § 7 ods. 1 zákona

[285] BARANCOVÁ, H., SCHRONK, R.: Pracovné právo. Druhé prepracované a doplnené vydanie. Bratislava: Sprint 2, 2013, str. 259, ISBN: 978-80-89393-97-8.
[286] Rozhodnutie Najvyššieho súdu ČR, sp.zn.: 21 Cdo 4596/2014 zo dňa 26.11.2015.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

o organizácii pracovného času v doprave a preto ich nemožno podľa tohto zákona považovať za mobilných zamestnancov. Na prvý pohľad by bolo možné uvedený legislatívny problém riešiť pomocou analógie legis, avšak aplikácia analógie legis v prospech vymedzenia pracoviska sa komplikuje v prípadoch, ak sa napríklad jedná o profesionálneho vodiča z povolania, ktorý má v pracovnej zmluve dohodnutý ako druh práce: „vodič – operátor“ alebo sa jedná o vodiča referenta, ktorý vedie služobné motorové vozidlo do 3,5t. na služobnej pracovnej ceste, ktorý nemá ako druh práce dohodnutú činnosť vedenie motorového vozidla. Ďalší aplikačný problém súvisí so žiakmi stredných škôl vykonávajúcimi dopravné činnosti a praktikantmi, pretože je otázne, či takéto subjektmi môžeme podradiť pod aplikáciu § 13 ods. 4 Zákonníka práce. Ustanovenia zákona o organizácii pracovného času v doprave o maximálnom pracovnom čase, o prestávkach v práci a o minimálnych dobách odpočinku mobilných zamestnancov v cestnej doprave sa síce vzťahujú aj na praktikantov a na žiakov stredných škôl vykonávajúcich dopravné činnosti, to však automaticky neznamená, že v zmysle § 7 ods. 1 zákona o organizácii pracovného času v doprave sa takéto subjekty považujú za mobilných zamestnancov, resp. za zamestnancov, ktorých má na mysli ustanovenie § 13 ods. 4 Zákonníka práce.

Monitorovanie zamestnanca prostredníctvom GPS systému pojmovo spadá pod monitorovanie zamestnancov v zmysle § 13 ods. 4 Zákonníka práce, v ktorom sú jednotlivé spôsoby monitorovania zamestnancov uvedené len príkladmo demonštratívnym výpočtom. Pred inštaláciou samotného technického zariadenia do dopravného prostriedku je zamestnávateľ povinný vopred informovať zamestnanca o inštalácii monitorovacieho zariadenia do dopravného prostriedku. Zamestnanec s jeho inštaláciou nemusí súhlasiť, avšak na monitorovanie zamestnanca sa v zmysle § 13 ods. 4 Zákonníka práce súhlas nevyžaduje. Táto skutočnosť však nevylučuje, že zamestnávateľ nebude potrebovať žiadny súhlas od zamestnanca. V súčasnej dobe nie je ničím výnimočným, že zamestnávateľ udelí súhlas na používanie súkromného motorového vozidla zamestnanca na pracovnoprávne účely. Pokiaľ má zamestnávateľ záujem o inštaláciu GPS systému do súkromného motorového vozidla zamestnanca, odporúčame, aby si zamestnávateľ so zamestnancom v samotnej dohode o používaní súkromného motorového vozidla zamestnanca na pracovnoprávne účely dohodli

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

možnosť inštalácie GPS systému a podmienky jeho využívania. Pokiaľ zamestnanec udelí zamestnávateľovi súhlas s inštaláciou GPS systému do svojho motorového vozidla, zamestnávateľ by mal vyhodnocovať údaje z GPS systému len v pracovnej dobe zamestnanca. Za týmto účelom môže byť GPS systém zo strany zamestnanca deaktivovaný prepnutím do režimu súkromná jazda, ak zamestnanec aktuálne využíva svoje súkromné motorové vozidlo po skončení jeho pracovnej doby. Pokiaľ by zamestnávateľ udelil vo vyššie uvedenej dohode o používaní súkromného motorového vozidla na pracovnoprávne účely zamestnancovi súhlas s využívaním motorového vozidla patriacej tretej osobe, mal by si zamestnávateľ zaobstarať súhlas aj od tejto tretej osoby, ktorá je vlastníkom motorového vozidla. Pokiaľ samotný GPS systém neobsahuje v sebe kamerový systém, ktorý umožňuje vyhotovovať z priestorov kabíny vodiča audiovizuálny záznam za účelom jeho spracovania a uschovania, zamestnávateľ nepotrebuje v zmysle zákona o ochrane osobných údajov súhlas zamestnanca ako dotknutej osoby. To však automaticky neznamená, že v prípade rozdielnej vnútroštátnej právnej úpravy inakšieho členského štátu Európskej únie by zamestnávateľ od svojho zamestnanca na území tohto členského štátu Európskej únie takýto súhlas so spracovaním osobných údajov nepotreboval a naopak.

V kontexte nami naznačených aplikačných problémov sa so zavádzaním GPS systému a následným monitorovaním zamestnancov v cestnej doprave na základe vyššie uvedeného ani zďaleka výpočet aplikačných problémov nekončí. Ďalší aplikačný problém súvisí s hmotnoprávnymi podmienkami uvedenými v § 13 ods. 4 Zákonníka práce, ktoré oprávňujú zamestnávateľa monitorovať zamestnanca. Pri zamestnancoch v cestnej doprave vystáva otázka, či môže zamestnávateľ monitorovať zamestnancov len počas ich pracovného času alebo aj v rámci doby odpočinku. Zákonník práce nám riešenie na tento aplikačný problém jednoznačne neposkytuje. Sme toho názoru, že pri skúmaní tohto aplikačného problému je potrebné každý jeden konkrétny prípad skúmať samostatne. Pokiaľ sa zamestnávateľ rozhodne monitorovať zamestnanca GPS systémom počas trávenia doby odpočinku, musí mať podľa nášho názoru vážny prevádzkový dôvod spočívajúci v osobitnej povahe činnosti zamestnávateľa, ktorý môže spočívať napríklad v prevencii pred neoprávneným odcudzením dopravného prostriedku alebo dodržiavaním bezpečnosti a ochrany zdravia pri práci

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zamestnanca. Sme však toho názoru, že v takomto prípade zásahu do súkromia zamestnanca by zamestnávateľ nemohol použiť ekonomický dôvod odôvodňujúci takýto zásah do súkromia zamestnanca. Z uvedeného dôvodu je dôležité, aby zamestnávateľ pri prerokovaní so zástupcami zamestnancov riadne odôvodnil dôvody, pre ktoré sa rozhodne monitorovať svojich zamestnancov. Pokiaľ by zamestnávateľ riadnym spôsobom neodôvodnil, prečo má záujem na monitorovaní zamestnancov aj počas doby odpočinku, takéto monitorovanie by bolo podľa nášho názoru v rozpore s § 13 ods. 4 Zákonníka práce. Obdobná situácia platí aj pri spolujazdcovi vodiča, ktorý počas jazdy vodiča čerpá pracovnú pohotovosť a je pripravený v prípade náhlej potreby viesť dopravný prostriedok za vodiča. Pokiaľ by sme pri riešení tohto aplikačného problému dospeli k právnemu záveru, že zamestnávateľ môže monitorovať pracovisko zamestnanca aj počas doby odpočinku aj počas čerpania pracovnej pohotovosti, vzniká nám otázka, ktorá časť kabíny kamióna tvorí pracovisko zamestnanca pracujúceho v cestnej doprave. Je celkom bežné, že kabína kamióna sa skladá z dvoch častí, pričom zadná časť kamióna je prispôsobená pre vodiča na trávenie prestávky v práci a dôb odpočinku, čo je odlišný časový úsek od pracovného času vodiča kamiónu. V aplikačnej praxi zadná časť kabíny kamióna je vybavená lôžkom, na ktorom vodič kamiónu trávi minimálny denný alebo týždenný odpočinok.

Ak je kabína vodiča kamiónu vybavená kamerovým systémom, ktorý môže byť súčasťou GPS systému, vzniká nám otázka, či môže zamestnávateľ monitorovať pracovisko zamestnanca aj vtedy, ak sa práve zamestnanec nenachádza v dopravnom prostriedku. Pri tomto aplikačnom probléme je potrebné zodpovedať otázku, či môže za istých okolností tvoriť kabína vodiča ako pracovisko zamestnanca súkromie zamestnanca bez jeho osobnej prítomnosti. Sme toho názoru, že môže, pokiaľ by súčasťou kabíny vodiča kamiónu boli veci, ktoré by umožnili zamestnávateľovi napríklad zistiť náboženské vyznanie alebo sexuálnu orientáciu zamestnanca. Zaujímavou otázkou zostáva použitie údajov zozbieraných z GPS systému a ich následné použitie na vyvodenie pracovnoprávnych dôsledkov voči zamestnancovi v podobe skončenia pracovného pomeru a ich prípustnosť v civilnom súdnom konaní ako jediného dôkazného prostriedku v konaní o neplatné skončenie pracovného pomeru.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

9.2.3 Informatívny merač rýchlosti

Medzi ďalší spôsob monitorovania zamestnancov v cestnej doprave patrí meranie maximálnej povolenej rýchlosti motorového vozidla, ktoré zamestnanec vedie po cestnej komunikácii. Najčastejšie sa jedná o meranie rýchlosti v areáli zamestnávateľa. Najčastejším dôvodom pre zavedenie maximálnej povolenej rýchlosti v areáli zamestnávateľa je zaistenie bezpečnosti a ochrany zdravia všetkých zamestnancov zamestnávateľa, pričom zamestnávateľ takýmto konaním prispieva k eliminácii hluku a prachu na jeho pracovisku ale aj vzniku pracovných úrazov z dôvodu kolízie motorového vozidla so zamestnancami v areáli zamestnávateľa. Nakoľko najčastejšou sankciou za porušenie maximálnej povolenej rýchlosti v areáli zamestnávateľa je vyvodenie pracovnoprávnych dôsledkov v podobe skončenia pracovného pomeru z dôvodu porušenia pracovnej disciplíny, považujeme za potrebné sa tomuto aplikačnému problému bližšie venovať.

Pokiaľ chce zamestnávateľ zaviesť vo svojom výrobnom areáli maximálnu povolenú rýchlosť, môže takúto povinnosť pre svojich zamestnancov stanoviť vo svojom vnútornom predpise, ktorým je dopravno-logistický poriadok a pracovný poriadok. S týmto pracovným poriadkom musia byť všetci dotknutý zamestnanci zamestnávateľa preukázateľným spôsobom v zmysle § 84 ods. 4 Zákonníka práce oboznámení. Zároveň by mal zamestnávateľ osadiť pri vstupe do svojho výrobného areálu informačné tabule, ktoré informujú zamestnancov o obmedzení maximálnej povolenej rýchlosti v areáli zamestnávateľa na cestných komunikáciách, ktoré sú vo vlastníctve zamestnávateľa. Zamestnávateľ môže zmerať maximálnu povolenú rýchlosť viacerými spôsobmi, pričom najčastejšie sa bude jednať o informačné merače rýchlosti s možnosťou vyhotovenia obrazového záznamu s tvárou vodiča.

Podľa aktuálnej právnej úpravy uvedenej v Zákonníku práce žiadny právny predpis nezakazuje takéto konanie zamestnávateľovi. V pracovnom poriadku môže zamestnávateľ stanoviť, že pokiaľ zamestnanec prekročí s motorovým vozidlom maximálnu povolenú rýchlosť, tak jeho konanie zakladá menej závažné porušenie pracovnej disciplíny alebo závažné porušenie pracovnej disciplíny, pričom hranicu medzi založením menej závažného porušenia pracovnej disciplíny a závažného porušenia pracovnej disciplíny by mal

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zamestnávateľ dostatočne jasne oddeliť a to prostredníctvom určenia hranice prekročenia rýchlosti jazdy v podobe kilometroch za hodinu. V prípade, ak zamestnanec opakovane poruší pracovnú disciplínu svojím zavineným konaním v podobe prekročenia maximálnej povolenej rýchlosti, takéto konanie môže viesť k vyvodeniu pracovnoprávnych následkov z pracovného pomeru v podobe výpovede z pracovného pomeru alebo okamžitého skončenia pracovného pomeru. V prípadnom civilnom súdnom konaní o neplatné skončenie pracovného pomeru by sa okrem podmienok zavedenia monitorovacieho zariadenia v zmysle § 13 ods. 4 Zákonníka práce a splnenia účinnosti vnútorného predpisu voči zamestnancom v zmysle § 84 ods. 4 Zákonníka práce určite skúmala kalibrácia samotného merača rýchlosti a zavinenie zamestnanca.

Pokiaľ by maximálnu povolenú rýchlosť prekročil zamestnanec zamestnávateľa na verejnej komunikácii a proti takémuto zamestnancovi by sa následne viedlo správne konanie pred príslušným dopravným inšpektorátom Policajného zboru Slovenskej republiky, zamestnávateľ môže za takéto konanie vyvodiť voči zamestnancovi pracovnoprávne dôsledky v podobe výpovede, ak takéto jeho konanie zakladá podľa vnútorného predpisu zamestnávateľa minimálne menej závažné porušenie pracovnej disciplíny. Ak sa v priebehu lehoty uvedenej v § 63 ods. 4 Zákonníka práce konanie zamestnanca, v ktorom možno vidieť porušenie pracovnej disciplíny stane predmetom konania iného orgánu, možno dať výpoveď ako aj okamžité skončenie pracovného pomeru ešte do dvoch mesiacov odo dňa, keď sa zamestnávateľ dozvedel o výsledku tohto konania. V zmysle súdnej praxe iným orgánom v zmysle § 63 ods. 4 Zákonníka práce treba rozumieť orgán, do právomoci ktorého patrí právomoc posudzovať konanie zamestnanca. Výsledkom konania môže byť v zmysle § 63 ods. 4 Zákonníka práce akékoľvek čo i len čiastkové zistenie iného orgánu, ktoré vyplýva z jeho právomoci.287 Nemusí ísť o záver, ktorý vyplýva z právoplatného rozhodnutia iného príslušného orgánu v zmysle § 63 ods. 4 Zákonníka práce.[288]

9.2.4 Ďalšie spôsoby monitorovania zamestnancov v cestnej doprave

[287] OLŠOVSKÁ, A.: Skončenie pracovného pomeru. Bratislava: Wolters Kluwer, 2015, str. 83, ISBN: 978-80-7552-001-2.
[288] Rozsudok Najvyššieho súdu Slovenskej republiky, sp. zn.: 3 Cdo 134/2005.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Ako bolo naznačené vyššie, medzi ďalšie spôsoby monitorovania zamestnancov v cestnej doprave patrí monitorovanie a kontrola prostredníctvom *mystery shoppingu* alebo prostredníctvom samotných cestujúcich. *Mystery shopping* možno charakterizovať ako kontrolu zamestnancov prostredníctvom utajenej identity. *Mystery shopping* ako kontrolu s utajenou identitou nemusí v aplikačnej praxi uskutočňovať len sám zamestnávateľ. Je celkom bežné, že zamestnávateľ poverí svojich vedúcich zamestnancov, aby v rámci utajenej identity ako cestujúci skontrolovali výkon práce vodičov dopravných prostriedkov. Na kontrolu svojich zamestnancov prostredníctvom utajenej identity si môže zamestnávateľ objednať rôzne špeciálne agentúry, ktoré za odplatu ponúkajú svoje služby pre zamestnávateľa tak, že anonymným spôsobom uskutočnia v dopravnom prostriedku pravidelné alebo náhodné kontroly zamerané na výkon práce vodičov alebo obsluhujúceho personálu dopravného prostriedku. Z takejto formy *„kontroly“* v súčasnej dobe profituje stále viac a viac agentúr. Z výkonu kontroly utajený cestujúci vyhotoví audiovizuálny záznam, ktorý odovzdá samotnému zamestnávateľovi. Pri takejto skrytej forme kontroly dochádza k spracovaniu osobných údajov bez vedomia zamestnanca, čím dochádza k narušeniu súkromia zamestnanca na pracovisku práve tým, že je utajeným spôsobom monitorovaný prostredníctvom tretích osôb. Takáto forma utajenej kontroly nemá v súčasnej dobe právny základ v Zákonníku práce. Zamestnávateľ je oprávnený sám alebo prostredníctvom svojich vedúcich zamestnancov kontrolovať výkon práce svojich zamestnancov, avšak nie prostredníctvom tretích osôb a súčasne menej invazívnymi spôsobmi kontroly, ktoré neporušujú základné ľudské právo zamestnanca na súkromný život. [289]

Ďalšiu formu kontroly zamestnancov pracujúcich v cestnej doprave uskutočňujú samotní cestujúci. Nie nadarmo sa medzi vodičmi autobusov hovorí, že: *„najväčším nepriateľom vodiča autobusu je jeho cestujúci“*. S plošným rozvojom internetizácie a s rozvojom nových aplikácií sa osobným cestným dopravcom otvárajú rôzne možnosti kontroly svojich zamestnancov práve prostredníctvom cestujúcich, ktorí majú spätnú možnosť ohodnotiť kvalitu služieb obsluhujúceho personálu dopravného prostriedku. Tým cestujúcim,

[289] BARANCOVÁ, H.: Nové technológie v pracovnom práve a ochrana zamestnanca (možnosti a riziká). Praha: Leges, 2016, str. 52 a 53, ISBN: 978-80-7502-176-2.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ktorí si zakúpili cestovný lístok cez internet majú možnosť dopravcovia zaslať dotazník kvality poskytovaných služieb. Cestujúci, ktorí si nekúpili cestovný lístok cez internet (dopravcovi nie je známa e-mailová adresa cestujúceho), majú možnosť ohodnotiť kvalitu služieb obsluhujúceho personálu dopravného prostriedku prostredníctvom rôznych aplikácií. Je pomerne bežnou skutočnosťou, že takého informácie sú podklad pre zamestnávateľa, ktorý sa na základe analýzy týchto výstupov rozhoduje, akým spôsobom tieto informácie ovplyvnia pracovnoprávny vzťah medzi zamestnancom a zamestnávateľom. V aplikačnej praxi je bežné, že pokiaľ sa na konkrétnej autobusovej linke vyskytne viacero sťažností na obsluhujúci personál dopravného prostriedku, zamestnávateľ vyvodí voči svojím zamestnancom pracovnoprávne postihy v podobe nepriznania mimoriadnej odmeny za príslušný kalendárny mesiac, alebo zamestnancovi uloží upozornenie za nepriaznivé plnenie pracovných úloh. Nie je ničím výnimočným, že tieto informácie získané priamo z mobilných aplikácií od samotných cestujúcich sú podkladom pre skončenie pracovnoprávneho vzťahu zamestnanca so zamestnávateľom.

Ďalším pomerne bežným spôsobom, ako zamestnávateľ môže voči zamestnancom v cestnej doprave uskutočniť výkon kontroly je prostredníctvom vykonania orientačnej dychovej skúšky zameranej na prítomnosť alkoholu v dychu zamestnanca. Takáto kontrola sa najčastejšie uskutočňuje v priestoroch zamestnávateľa a môže ju vykonať samotný zamestnávateľ alebo ním poverený vedúci zamestnanec. Najčastejším subjektom výkonu kontroly sú vodiči dopravných prostriedkov, pričom s rozvojom palubných služieb nie je vylúčené, že sa vykonaniu takejto dychovej skúšky zameranej na prítomnosť alkoholu v dychu môže podrobiť okrem vodiča dopravného prostriedku aj celý palubný personál. Právnym základom pre uskutočnenie výkonu takejto kontroly tvorí zákon č. 124/2006 Z.z. o bezpečnosti a ochrane zdravia pri práci v znení neskorších predpisov (ďalej len: „zákon o BOZP“). Podľa § 12 ods. 1 pís. l) zákona o BOZP je zamestnanec povinný sa podrobiť vyšetreniu, ktoré vykonáva zamestnávateľ alebo príslušný orgán štátnej správy, aby zistil, či zamestnanec nie je pod vplyvom alkoholu, omamných látok alebo psychotropných látok. Okruh zamestnancov zamestnávateľa a iných osôb oprávnených dať zamestnancovi pokyn, aby sa podrobil vyšetreniu, uvedie zamestnávateľ v pracovnom poriadku alebo vo vnútornom predpise.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Dychovú skúšku môže zamestnanec odmietnuť iba v prípade, že má lekárske potvrdenie o závažnej prekážke, ktorá znemožňuje súvislý výdych do alkohol testera. Takouto závažnou prekážkou môže byť napríklad ťažká astma. Niektoré alkohol testery však stačí priložiť k ústam zamestnanca a na vykonanie dychovej skúšky nie je potrebný súvislý výdych do alkohol testeru. Pokiaľ výkon kontroly neuskutočňuje priamo zamestnávateľ ale napríklad vedúci zamestnanec, mal by zamestnávateľ takouto činnosťou písomne poveriť konkrétneho zamestnanca, ak takéto písomné poverenie nie je súčasťou vnútorného predpisu alebo pracovného poriadku. Pri vykonaní dychovej skúšky zameranej na prítomnosť alkoholu v dychu zamestnanca by mal byť prítomný aspoň jeden nezávislý svedok a o výsledku kontroly by mala byť spísaná zápisnica alebo protokol o vykonaní dychovej skúšky. Pokiaľ je to z personálnych dôvodov možné, odporúčame, aby nezávislým svedkom pri dychovej skúške bol práve zástupca zamestnancov pre bezpečnosť a ochranu zdravia pri práci. Je bežnou praxou, že z dôvodu právnej istoty sa zvykne orientačná dychová skúška opakovať s odstupom minimálne desiatich minút, pričom sa zvyknú vykonať až tri dychové skúšky. Pokiaľ zamestnanec s výsledkom dychovej skúšky nesúhlasí, mal by dobrovoľne vyhľadať spolu s prítomnými osobami zdravotnícke zariadenie, ktoré tomuto zamestnancovi odoberie biologický materiál na zistenie prítomnosti alkoholu v jeho tele. Protokolu o vykonaní dychovej skúšky je potrebné venovať náležitú pozornosť, pretože najčastejšie býva jedinými dôkazným prostriedkom v konaní o neplatné skončenie pracovného pomeru. V nedávnej dobe sa v pomerne ostro kritizovanom rozhodnutí k problematike alkoholu na pracovisku vyjadril Najvyšší súd Českej republiky. V prejednávanom prípade bol zamestnancovi pred začiatkom pracovnej zmeny zistený alkohol vo výške 0,32 promile alkoholu, pri druhej duchovej skúške o pol hodiny neskôr 0,23 promile alkoholu a pri odbere krvi vo večerných hodinách 0,11% promile alkoholu v krvi. Zamestnancovi bola následne udelená výpoveď pre závažné porušenie pracovnej disciplíny. Najvyšší súd Českej republiky po preskúmaní všetkých okolností prípadu došiel k záveru, že samo o sebe požitie alkoholu zamestnancom nemusí vždy automaticky znamenať závažné porušenie pracovnej disciplíny, aby mohol byť so zamestnancom okamžite skončení pracovný pomer. Pozitívne zistenie alkoholu v krvi zo strany zamestnávateľa nezakladá automaticky na strane zamestnanca závažné porušenie pracovnej disciplíny, pre ktoré by mohol dať zamestnávateľ zamestnancovi okamžité skončenie pracovného

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

pomeru.290 Najvyšší súd Českej republiky v predmetom rozhodnutí poukázal na hľadiská, ktoré musia byť pri hodnotení miery závažnosti konania zamestnanca brané v úvahu. Takýmto hľadiskom je funkcia, ktorú zamestnanec zastáva, postoj k plneniu pracovných úloh, doba a situácia, za ktorých došlo k porušeniu právnych prepisov, miera zavinenia zamestnanca, spôsob a intenzita porušenia konkrétnych povinností zamestnanca, či svojím konaním spôsobil zamestnancovi škodu a pod.[291]

9.2.5 Verejný záujem

Zákonník práce nepozná pojem verejný záujem. Verejný záujem je z pohľadu práva neurčitým právnym pojmom. Verejný záujem predstavuje hodnotu, ktorá je niekedy nadradená nad základné ľudské právo a inokedy, podľa povahy záujmu, je nadradený nad viaceré základné práva a slobody. V prípade niekoľkých dotknutých základných práv možno vyvodiť, že existenciu verejného záujmu na obmedzení jedného základného práva vylučuje preskúmanie na obmedzení ďalšieho základného práva.292 V danom prípade je potrebné sa spýtať, či neexistuje verejný záujme na tom, aby boli za každých okolností dodržiavané právne predpisy zaisťujúce účastníkom premávky na pozemných komunikáciách ich bezpečnosť ? Pripomíname, že spomedzi viacerých dôvodov odôvodňujúcich zásah do súkromia zamestnancov v cestnej doprave je zvýšený záujem na tom, či sa v aplikačnej praxi dodržiavajú ustanovenia o maximálnom dennom pracovnom čase, doby odpočinku, bezpečnostné prestávky alebo maximálne povolenú rýchlosť na pozemnej komunikácií.

V prípade, ak by došlo k vyvodeniu pracovnoprávnej zodpovednosti voči zamestnancovi v cestnej doprave v podobe skončenia pracovného pomeru z dôvodu porušenia pracovnej disciplíny na podklade dôkazu z neoprávneného monitorovania zamestnanca v zmysle § 13 ods. 4 Zákonníka práce, je na zvážení súdu, či takýto dôkaz v rámci individuálneho pracovnoprávneho sporu v rámci možnej dôkaznej núdze pripustí a následne vo veci právoplatne rozhodne. Sme však toho názoru, že v takomto prípade je potrebné aj

290 Rozsudok Najvyššieho súdu Českej republiky, sp. zn: 21Cdo 4733/2015.
291 Dostupné na: https://www.epravo.cz/top/clanky/je-alkohol-na-pracovisti-vzdy-duvodem-k-vypovedi-105684.html. (prezerané dňa 16.09.2023)
292 DRGONEC, J.: Ústava Slovenskej republiky. Komentár. Teória a prax. 1. vyd. Bratislava: C.H. Beck, 2015, str. 538, ISBN: 978-80-89603-39-8.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zvážiť vyššie uvedený verejný záujem celej spoločnosti na tom, aby sa profesionálni zamestnanci v cestnej doprave nedopúšťali konaní (napr. aj porušovania pracovnoprávnych inštitútov ako napríklad prestávok v práci a dôb odpočinku) pri premávke na pozemných komunikáciách. Súčasne sme toho názoru, že nie každé rozhodnutie týkajúce sa prítomnosti alkoholu v krvi zamestnanca na základe vykonanej skúšky je priamo aplikovateľné aj na zamestnancov pracujúcich vo verenej, resp. v cestnej doprave. Nakoľko máme v zmysle príslušných predpisov na SR nulovú toleranciu v otázke prítomnosti alkoholu v krvi vodičov vedúcich cestné motorové vozidlá na pozemných komunikáciách, zastávame názor, že nie je možné na profesionálnych vodičov v cestnej doprave v otázke prítomnosti alkoholu v krvi a následného vyvodenia pracovnoprávnych dôsledkov otrocky aplikovať súdneho rozhodnutia najvyšších súdnych autorít, ktorých podstatou je *„neposvätenie nulovej tolerancie prítomnosti alkoholu v krvi zamestnanca na pracovisku v kontexte závažného porušenia pracovnej disciplíny a následne vyvodenia pracovnoprávnych dôsledkov v podobe okamžitého skončenia pracovného pomeru.“* V tejto súvislosti pripomíname, že uvedení zamestnanci v cestnej doprave musia byť uzrozumení s tým, že sa na nich ako profesionálnych vodičov v cestnej doprave kladnú zvýšené nároky v otázke bezpečnosti a tým pádom musia byť uzrozumení s tým, že intenzita ich monitorovania môže byť v určitých aspektoch zvýšená a ospravedlnená častejšími kontrolami zameranými na bezpečnosť v cestnej doprave. Je to dané charakterom výkonu práce a všeobecným záujmom spoločnosti nad bezpodmienečným dodržiavaním predpisov zaisťujúcich bezpečnosť premávky na pozemných komunikáciách.

9.3 OCHRANA SÚKROMIA SUDCOV

Treťou osobitnou kategóriou zamestnancov, na ktorú sa zmeriame v našej vedeckej analýze pri skúmaní ich práva na ochranu súkromia, sú sudcovia všeobecných súdov. Sudcovia všeobecných súdov tvoria osobitnú kategóriu zamestnancov preto, pretože ich právny vzťah k štátu sa považuje za osobitný právny vzťah *sui generis*, na ktorý sa však aplikujú vybrané inštitúty typické pre pracovné právo, ako napríklad pracovný čas, dovolenka, prekážky v práci a pod. Výnimkou nie je v tomto smere ani právna ochrana súkromia sudcov, avšak s určitými špecifickými odchýlkami typickými pre tento typ výkonu povolania.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Podľa nálezu Ústavného súdu SR sp. zn. II. ÚS 184/2015 zo dňa 11. novembra 2015 platí, že: *„voľnočasová aktivita sudcu, zvlášť ak ide o poľovníctvo, ktoré má významný sociálny rozmer, môže byť predmetom legitímneho záujmu médií, pričom skutočnosť, že ide o voľnočasovú aktivitu, nemôže byť sama osebe dôvodom na uprednostnenie ochrany súkromia sudcu pred ochranou slobody prejavu médií. Z hľadiska intenzity ochrany súkromia požíva predseda súdu nižšiu mieru ochrany ako ostatní sudcovia príslušného súdu, keďže predseda súdu symbolizuje súd, na čele ktorého stojí, zastupuje ho a reprezentuje navonok. To platí zvlášť vtedy, ak ide o funkciu predsedu Špecializovaného trestného súdu, ktorý symbolizuje boj s korupciou.“*[293] V prejednávanom prípade zažaloval sudca predmetný denník prostredníctvom žaloby na ochranu osobnosti za to, o ňom uviedol údajné neoprávnené informácie o jeho osobe v článkoch, ktoré malo zasiahnuť do jeho cti, ľudskej dôstojnosti, dobrého mena, povesti a súkromia. V rámci predmetnej žaloby žiadal ospravedlnenie a náhradu nemajetkovej ujmy v peniazoch. Okresný súd Banská Bystrica vydal čiastočný rozsudok, ktorým zaviazal sťažovateľku v lehote 15 dní od právoplatnosti rozhodnutia uverejniť v strede hornej polovice titulnej strany denníka v troch po sebe nasledujúcich vydaniach ospravedlnenie veľkými písmenami abecedy v znení petitu navrhnutého žalobcom. Okresný súd o náhrade nemajetkovej ujmy a o náhrade trov konania čiastočným rozsudkom nerozhodol. Na základe odvolania sťažovateľa označené rozhodnutie okresného súdu potvrdil krajský súd napadnutým rozsudkom. O dovolaní sťažovateľky proti napadnutému rozsudku krajského súdu rozhodol najvyšší súd napadnutým uznesením tak, že ho odmietol.

V rámci rozhodovania sa musel Ústavný súd SR vysporiadať na jednej strane s právom denníka na slobodu prejavu a na druhej strane s právom sudcu na ochranu súkromia. Ťažiskovým predmetom sa stalo teda právne váženie práva na slobodu prejavu denníka slobodne informovať o mimopracovných aktivitách sudcu a práva sudcu na ochranu súkromia pred nezákonným zásahom printového média. Ústavný súd preto pristúpil k preskúmaniu proporcionality medzi zásahom do slobody prejavu sťažovateľky a ústavnými garanciami práva na súkromie žalobcu. Na ten účel, obdobne ako v iných porovnateľných prípadoch (napr. II. ÚS 152/08, II. ÚS 326/09, I. ÚS 408/2010, IV. ÚS 492/2012), ústavný súd vykonal test

[293] Nález Ústavného súdu SR sp. zn. II. ÚS 184/2015 zo dňa 11. novembra 2015

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

proporcionality založený na hľadaní odpovedí na otázky KTO, O KOM, ČO, KDE, KEDY a AKO v danom prípade *„hovoril“* (uverejnil informáciu).

Z judikatúry ESĽP vyplýva, že privilegované postavenie z hľadiska ochrany slobody prejavu patrí novinárom a masmédiám, a to zvlášť pri informovaní o veciach verejného záujmu (napr. rozsudok ESĽP Prager a Oberschlick v. Rakúsko z 26. 4. 1995, sťažnosť č. 1594/90, alebo rozsudok ESĽP Bladet Tromso a Stensaas proti Nórsku z 20. 5. 1999, sťažnosť č. 21980/93). Novinári majú (sociálnu) povinnosť poskytovať informácie a myšlienky týkajúce sa všetkých záležitostí verejného záujmu a verejnosť má právo takéto informácie dostať. Novinárom je dokonca umožnené používať určitú mieru preháňania a provokácie (Perna v. Taliansko, sťažnosť č. 48898/99, rozsudok ESĽP zo 6. 5. 2003, bod 39).

Dôsledkom snahy o podporu výmeny názorov o verejne zaujímavých témach je aj kategorizácia osôb, ktorých sa informácie uvedené v tlači týkajú a do ktorých osobnostnej sféry negatívne zasahujú, resp. môžu zasahovať. Hranice akceptovateľnosti šírenia informácií týkajúcich sa osobnostnej sféry sú najširšie u politikov a najužšie u *„bežných“* občanov. Žalobca bol v čase publikovania inkriminovaných článkov sudcom Špecializovaného trestného súdu, pričom v predchádzajúcom období bol predsedom Špeciálneho súdu (právneho predchodcu Špecializovaného trestného súdu) a v období bezprostredne predchádzajúcom času, keď boli inkriminované články publikované, aj verejne pripustil, že sa bude opätovne uchádzať o funkciu predsedu Špecializovaného trestného súdu, pričom v konečnom dôsledku bol do tejto funkcie aj opätovne ustanovený. V nadväznosti na uvedené skutočnosti ústavný súd pripomína, že vo svojej judikatúre už vyslovil právny názor, v zmysle ktorého v línii od verejne neznámych jednotlivcov po politikov sa sudcovia z hľadiska intenzity ochrany osobnosti nachádzajú uprostred s miernou tendenciou smerujúcou k politikom (m. m. II. ÚS 152/08 bod 31, pozri tiež II. ÚS 261/06 uverejnené aj v ZSP 1/2007 pod č. 36/2007 na s. 426). Ústavný súd tento záver v konkrétnych okolnostiach posudzovanej veci považuje za žiaduce nielen zdôrazniť, ale aj doplniť v tom smere, že: ***„z hľadiska intenzity ochrany súkromia je potrebné diferencovať medzi predsedom súdu a ostatnými sudcami príslušného súdu, ktorí požívajú nepochybne vyššiu mieru ochrany svojho súkromia ako predseda súdu, ktorý symbolizuje príslušný súd, na čele ktorého stojí a ktorý zastupuje a reprezentuje navonok, pričom už tým,***

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

že sa o túto funkciu uchádza, si musí byť vedomý, že bude vystavený zvýšenej pozornosti printových i elektronických médií.“

Podľa uvedeného nálezu Ústavného súdu SR: *„sudca tiež nemôže podľa Ústavného súdu paušálne žiadať o utajenie údajov o svojej osobe. To mu v určitej miere garantuje zákon o sudcoch, ale podľa Ústavného súdu musí mať na takéto utajenie akceptovateľné dôvody.“* Zverejnenie ospravedlnenia v tlači, ktoré predstavuje neprípustný zásah do slobody prejavu, bolo nezvratné, a tak Ústavný súd SR ako kompenzáciu určil finančné zadosťučinenie 3.000,- Eur.

Na základe nálezu Ústavného súdu SR vyplýva, že je legitímne, aby médiá vyjadrili svoje pochybnosti a podozrenia, ak konajú v snahe informovať verejnosť o veci verejného záujmu. Ústavný súd konštatoval, že aj súkromná sféra sudcov môže byť predmetom kritiky a ich voľnočasové aktivity môžu byť predmetom legitímneho záujmu médií. V rámci uvedeného nálezu Ústavného súdu prevážilo právo na slobodu prejavu médií pred právom na ochranu súkromia sudcu.

V poradím druhým prípadom týkajúcim sa práva na ochranu rodinného a súkromného života v spojení s právom na ochranu súkromia je mediálne známy prípad sudkyne Špecializovaného trestného súdu a novinárky predmetného denníka. V prejednávanom prípade pred Súdnou radou SR vystala právna otázka, či vzájomný vzťah sudkyne a novinárky je súčasťou práva na ochranu rodinného a súkromného života v spojení s právom na ochranu súkromia a z uvedeného dôvodu nie je daný dôvod na jeho bližšie skúmanie a právne dôsledky z neho vyplývajúce na samotnú rozhodovaciu činnosť sudkyne, alebo práve naopak, verejná diskusia o tomto súkromnom vzťahu sudkyne a novinárky je legitímnou verejnou diskusiou a je daný dôvod na jeho bližšie skúmanie za účelom odstránenia akýchkoľvek pochybností ohľadom nestranného rozhodovania sudkyne. Z vyhlásenia Združenia sudcov Slovenska k právu sudcu na ochranu jeho súkromia vyplýva, že: *„Právo každého na rešpektovanie jeho súkromného a rodinného života je jedným z kľúčových pilierov demokratickej spoločnosti a základnou podmienkou jej pokroku, keďže predstavuje záruku rozvoja osobnosti každého jednotlivca bez vonkajších zásahov v jeho vzťahoch s inými ľudskými bytosťami. Toto základné právo patrí nepochybne aj každému sudcovi a sudkyni. Miera jeho ochrany je však v ich prípade*

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

užšia. Je to dané tým, že nestačí, ak sú sudcovia subjektívne schopní nestranne konať a rozhodovať, ale rovnako dôležité je, aby tak boli aj vnímaní. Nevyhnutne totiž potrebujú dôveru verejnosti v ich nezávislosť a nestrannosť, aby mohli úspešne vykonávať svoje povinnosti a zachovať autoritu súdnictva pri riešení právnych sporov alebo pri rozhodovaní o vine alebo nevine osoby v trestnom konaní. Táto požiadavka sa odráža v zákonnej povinnosti každého sudcu a sudkyne aj v občianskom živote (dokonca i po skončení výkonu funkcie) zdržať sa všetkého, čo by mohlo narušiť vážnosť a dôstojnosť funkcie sudcu/sudkyne alebo ohroziť dôveru v nezávislé, nestranné a spravodlivé rozhodovanie súdov. Z tohto pohľadu považuje Združenie sudcov Slovenska aktuálne prebiehajúcu verejnú diskusiu o možnom dopade vzťahu exponovanej sudkyne a mienkotvornej novinárky, ktorý má súkromný charakter, na nestrannosť súdneho rozhodovania za plne legitímnu."[294] Naopak predseda Súdnej rady SR nevidel dôvod na bližšie skúmanie tohto súkromného vzťahu pred Súdnou radou SR s odôvodnením, že: *„Súdna rada SR nie je oprávnená vstupovať do súkromia a rodinných vzťahov žiadneho sudcu. Na tom nič nemení to, že ide o rodinný vzťah medzi známou novinárkou a významnou sudkyňou. Vzťah sudkyne a novinárky je rodinný vzťah, ktorý je chránený v Charte základných práv EÚ, teda Súdnym dvorom EÚ. Každý právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie. Charta základných práv má prednosť pred naším základným zákonom a rozsudky Súdneho dvora sú záväzné aj pre Slovensko. Podobne je formulovaná i ochrana rodinných vzťahov v Dohovore o ochrane ľudských práv a základných slobôd a v judikatúre Európskeho súdu pre ľudské práva. Poukázal tiež na ochranu súkromia a rodinného života vyplývajúcu z Ústavy SR. Bolo by totiž nanajvýš nevhodné a nešťastné, ak by sa Súdna rada ako ústavný orgán sudcovskej legitimity dostala do pozície porušovateľky základných a ľudských práv garantovaných ústavou a medzinárodnými záväzkami Slovenskej republiky."* [295]

Na základe vyššie uvedených príkladov z aplikačnej praxe možno dospieť k právnemu záveru, že miera ochrany práva na súkromie sudcov bude v porovnaní s inými občanmi SR

[294] Dostupné na internete: http://www.pravnelisty.sk/clanky/a1269-vyhlasenie-zdruzenia-sudcov-slovenska-k-pravu-sudcu-na-ochranu-jeho-sukromia. (Prezerané dňa 25.10.2023, 15:25 hod.)

[295] Dostupné na internete: https://www.sudcovia.sk/sk/clanky/18-clanky/246-j-mazak-nevidi-dovod-aby-sa-vztahom-p-zaleskej-zaoberala-sudna-rada. (Prezerané dňa 25.10.2023, 16:15 hod.)

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

nižšia z dôvodu verejného záujmu v nezávislé a nestranné rozhodovanie sudcov v rámci justície. Konkrétnu kolíziu práva na ochranu súkromia sudcov a práva na slobodu slova bude potrebné v každom jednom prípade posudzovať individuálne, veľmi citlivo a dôsledne tak, aby uplatnením jedného práva nedošlo k výraznému narušeniu druhého práva. Bude úlohou súdov, aby každé jedno narušenie práva na ochranu súkromia odôvodnené právom na slobodu prejavu tretej osoby prešlo testom legality, legitimity a proporcionality tak, aby napokon *„tzv. víťazné právo“* malo svoj zákonný a riadne odôvodnený podklad v samotnom rozhodnutí súdu.

Podľa § 34 ods. 6 a ods. 7 zákona č. 385/2000 Z. z. zákon o sudcoch v znení neskorších predpisov platí, že: *„Sudca má v odôvodnených prípadoch právo na zabezpečenie ochrany svojej osoby, svojich rodinných príslušníkov a svojho obydlia, ak o to správu súdu požiada; takisto má právo na bezplatné poskytnutie primeraných prostriedkov na zabezpečenie ochrany alebo náhrady nákladov takej ochrany. Bez súhlasu sudcu nemožno zverejňovať jeho tvár a bydlisko; to sa vzťahuje aj na rodinných príslušníkov sudcu, ak je to potrebné na účinnú ochranu sudcu a jeho rodiny a rodinní príslušníci s tým súhlasia. Sudca má právo aj na primerané utajenie údajov o jeho osobe a jeho rodine.“* Uvedené predstavuje základné práva sudcu. Uvedené ustanovenia predstavujú špeciálne ustanovenia týkajúce sa ochrany súkromia a osobných údajov sudcu a jeho členov rodiny pri výkone svojej funkcie. Uvedené ustanovenie v zákone o sudcoch predstavuje zvýšenú ochranu práva na súkromie a na ochranu osobnosti pri vyhotovovaní obrazových a zvukovoobrazových záznamov tváre sudcu bez jeho súhlasu v situácii, keď to odôvodňujú konkrétne okolnosti prejednávaného prípadu. Najčastejšie pôjde o skoršie vyhrážky o fyzickej likvidácii sudcu a jeho člena rodiny, pokiaľ rozhodne v neprospech vyhrážateľa.

9.4 ZÁKON O SLOBODNOM PRÍSTUPE K INFORMÁCIÁM A OCHRANA OSOBNÝCH ÚDAJOV ZAMESTNANCOV ORGÁNOV VEREJNEJ MOCI (POVINNÝCH OSÔB)

V rámci tejto kapitoly sa budeme venovať osobitnej situácii ochrany osobných údajov zamestnancov orgánov verejnej moci, a to z toho dôvodu, že v ich prípade právna úprava národného právneho poriadku upravuje osobitné pravidlá ochrany. Tie sú zakotvené

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

v infozákone,[296] ktorý všeobecne upravuje podmienky, postup a rozsah slobodného prístupu k informáciám v nadväznosti na čl. 26 a 45 Ústavy Slovenskej republiky.

Vzhľadom na základný princíp infozákona, ktorý spočíva v podobe princípu čo nie je tajné, je verejné[297] by malo platiť pravidlo, že orgány verejnej správy informujú aj o údajoch, ktoré tvoria osobné údaje svojich zamestnancov. Z daného dôvodu infozákon ako prejav princípu proporcionality upravuje aj zákonné obmedzenia prístupu k informáciám. Jedno z daných obmedzení tvorí práve aj ochrana osobných údajov (§ 9 infozákona).

V predmetnej kapitole vymedzíme princípy infozákona, v krátkosti kto postupuje podľa tohto zákona čo je to informácia a napokon výnimky zo sprístupnenia informácií z dôvodu ochrany osobných údajov z pohľadu zákona a súdnej judikatúry.

9.4.1 Princípy infozákona

Ústavné právo na prístup k informáciám je z pohľadu zákonnej právnej úpravy bližšie rozvinuté v infozákone. Infozákon je vybudovaný na základe viacerých princípov, ktoré vo svojej postate napomáhajú naplniť všeobecný princíp verejnej správy – princíp transparentnosti.[298]

Základným princípom infozákona je princíp „čo nie je tajné, je verejné“.[299] Ide tu o prejav princípu transparentnosti verejnej správy.[300]

Okrem tohto princípu ešte z textu zákona možno vyabstrahovať aj nasledujúce princípy, a to:

a) princíp aktívneho sprístupnenia informácií,

b) princíp sprístupnenia informácií na základe žiadosti,

c) princíp bezplatného sprístupnenia informácií,

---

[296] Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov (ďalej aj ako „inforzákon“ alebo „ZSI“).
[297] Pozri ďalej v texte.
[298] Napríklad Košičiarová, S. Správne právo hmotné. Všeobecná časť. Plzeň : Aleš Čeněk, 2022, s. 90 alebo Horvat, M. In Cepek, B. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : Wolters Kluwer, 2018, s. 74.
[299] Porovnaj Wilfling, P. Zákon o slobodnom prístupe k informáciám. Komentár. Problémy z praxe. Rozhodnutia súdov. Pezinok : Via Iuris, 2012, s. 48.
[300] Ikrényi, P. a kol. Zákon o slobodnom prístupe k informáciám. Komentár. Bratislava : Wolters Kluwer, 2015, s. 23.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

d) princíp sprístupnenia informácií bez uvedenia dôvodu.

Princíp čo nie je tajné, je verejné, vyplýva z čl. 26 ods. 1 Ústavy SR, má teda svoj ústavnoprávny rozmer. Podstata tohto princípu znamená, že subjekty, ktoré zaťažuje informačná povinnosť (povinné osoby), sú povinné sprístupňovať všetky informácie, ledaže by zákon ustanovil inak. Prejav tohto ústavného princípu v texte infozákona možno vidieť najmä v texte § 3 ods. 1[301] a § 12.[302] Výnimky z jeho uplatnenia potom vyplývajú najmä z § 8 až 11a[303] infozákona, ale aj napríklad z § 3 ods. 2.[304]

Výpočet dôvodov obmedzenia sprístupnenia informácií je pritom len demonštratívny. Ďalšie dôvody môžu vyplývať aj z osobitných právnych predpisov. To reflektuje vo svojej rozhodovacej činnosti aj Ústavný súd SR, podľa ktorého: „Vo všeobecnej rovine preto ústavný súd uzatvára, že pre obmedzenie základného práva na prístup k informáciám nie sú relevantné len ustanovenia § 8 až § 11 zákona o slobode informácií explicitne vymedzujúce obmedzenia v prístupe k informáciám, ale aj ustanovenia iných zákonných právnych predpisov chrániace práva a slobody iných, bezpečnosť štátu, verejný poriadok, verejné zdravie a mravnosť. Ústavný súd sa tak stotožňuje s názorom sťažovateľa, že zákon o slobode informácií je výrazom zásady ‚čo nie je tajné, je verejné', avšak rozsah toho, čo je ‚tajné', nemusí nevyhnutne

[301] Každý má právo na prístup k informáciám, ktoré majú povinné osoby k dispozícii. Právo na prístup k informáciám sa nevzťahuje na informácie, ktoré nie sú k dispozícii, najmä na vytváranie výkladových stanovísk, rozborov, analýz, referátov, odborných stanovísk, politických stanovísk, prognóz a výkladov právnych predpisov a na vytváranie názorov.

[302] Všetky obmedzenia práva na informácie vykonáva povinná osoba tak, že sprístupní požadované informácie vrátane sprievodných informácií po vylúčení tých informácií, pri ktorých to ustanovuje zákon. Oprávnenie odmietnuť sprístupnenie informácie trvá iba dovtedy, kým trvá dôvod nesprístupnenia.

[303] Ochrana utajovaných skutočností, ochrana osobnosti a osobných údajov, ochrana obchodného tajomstva, obmedzenie prístupu k informáciám pri ochrane pred ujmou v hospodárskej súťaži, ďalšie obmedzenia prístupu k informáciám.

[304] Povinná osoba podľa § 2 ods. 3 sprístupní iba informácie o hospodárení s verejnými prostriedkami, nakladaní s majetkom štátu majetkom vyššieho územného celku alebo majetkom obce, o životnom prostredí, o úlohách alebo odborných službách týkajúcich sa životného prostredia a o obsahu, plnení a činnostiach vykonávaných na základe uzatvorenej zmluvy. Toto obmedzenie povinnosti sprístupňovať informácie sa nevzťahuje na povinné osoby podľa § 2 ods. 3, v ktorých majú povinné osoby podľa § 2 ods. 1 a 2 samostatne alebo spoločne výlučnú priamu alebo nepriamu účasť.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

vyplývať len zo zákona o slobode informácií.“[305] Príkladom môže byť § 3 ods. 12 zákona č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.[306]

Princíp aktívneho sprístupňovania informácií má svoj predobraz v čl. 26 ods. 5 Ústavy SR[307] a vo vzťahu k národnostným menšinám aj v čl. 34 ods. 1.[308] Tento princíp je pretavený predovšetkým do podoby § 5 (vymedzenie okruhu informácií a konkrétnych povinných osôb, ktoré ich zverejňujú, a to predovšetkým prostredníctvom hromadného prístupu, t. j. najmä za využitia siete internet), § 5a (vymedzenie okruhu povinne zverejňovaných zmlúv uzatváraných povinnými osobami, ktoré bez zverejnenia nemôžu nadobudnúť účinnosť) a § 5b (ide najmä o povinne zverejňované faktúry) infozákona, ktorý upravuje povinné zverejňovanie informácií. Národnostné menšiny a ich prístup k informáciám sú potom upravené najmä v § 6 ods. 5 a § 16 ods. 8 infozákona.

Princíp sprístupnenia informácií na základe žiadosti (tzv. pasívne zverejňovanie informácií) má svoj ústavnoprávny rozmer odvoditeľný z čl. 26 ods. 1 Ústavy SR, podľa ktorého sa právo na informácie zaručuje. V rovine infozákona je tento princíp pretavený primárne do § 14 (sprístupňovanie informácií na základe žiadosti) a § 21d (sprístupnenie informácií na účely opakovaného použitia na základe žiadosti).

Vzťah medzi princípom sprístupnenia informácií na základe žiadosti a princípu aktívneho sprístupňovania informácií je taký, že informácie, ktoré nie sú zo zákona sprístupňované aktívne a ktorými zároveň disponuje povinná osoba, sa sprístupnia na základe žiadosti, ak tu neexistuje prekážka sprístupnenia (napr. § 8 až 11a infozákona). Oba tieto princípy sú preto nevyhnutným dôsledkom a prejavom základného princípu infozákona – princípu čo nie je tajné, je verejné.

---

[305] Uznesenie Ústavného súdu SR sp. zn. III. ÚS 96/2010-14 z 9. marca 2010, s. 10.
[306] Slovenská technická norma a technická normalizačná informácia sa nesprístupňuje podľa osobitného predpisu okrem slovenskej technickej normy podľa § 12 ods. 2.
[307] Orgány verejnej moci majú povinnosť primeraným spôsobom poskytovať informácie o svojej činnosti v štátnom jazyku.
[308] Občanom tvoriacim v Slovenskej republike národnostné menšiny alebo etnické skupiny sa zaručuje všestranný rozvoj, najmä právo spoločne s inými príslušníkmi menšiny alebo skupiny rozvíjať vlastnú kultúru, právo rozširovať a prijímať informácie v ich materinskom jazyku, združovať sa v národnostných združeniach, zakladať a udržiavať vzdelávacie a kultúrne inštitúcie.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Princíp bezplatného sprístupnenia informácií znamená, že povinná osoba nemôže podmieniť sprístupnenie informácie zaplatením správneho poplatku. Bezplatné sprístupnenie informácie reflektuje infozákon v § 21 ods. 1 a na účely opakovaného použitia aj v § 21k ods. 1. Výnimku z tohto pravidla musí ustanoviť zákon (pozri § 21k ods. 2 a 3). Túto skutočnosť reflektuje aj zákon č. 145/1995 Z. z. o správnych poplatkoch, podľa ktorého od poplatkov sú oslobodené úkony súvisiace s vykonávaním všeobecne záväzných právnych predpisov o slobodnom prístupe k informáciám.[309]

V rozpore s týmto princípom nie je ani tá skutočnosť, že povinná osoba môže požadovať zaplatenie materiálnych nákladov, ktoré jej vzniknú v súvislosti so sprístupnením informácie. Podľa súdnej judikatúry: „Obmedziť právo na sprístupnenie informácií je teda možné len zo zákonom ustanovených dôvodov. Nezaplatenie finančnej úhrady materiálnych nákladov vopred nie je podľa zákona o slobode informácií dôvodom na obmedzenie prístupu k informáciám. Z procesu sprístupňovania informácií, ktorý je upravený v ust. § 14 a nasl. cit. zákona nevyplýva pre povinnú osobu možnosť nerozhodnúť o žiadosti o informáciu alebo informáciu nesprístupniť z dôvodu, že žiadateľ vopred nezaplatil finančnú úhradu nákladov. Zaplatenie finančnej úhrady vopred nie je podľa zákona podmienkou ďalšej činnosti štátneho orgánu. (...) Podľa ust. § 17 ods. 1 zákona o slobode informácií žiadosť o sprístupnenie informácie povinná osoba vybaví bez zbytočného odkladu, najneskôr do 10 dní od podania žiadosti.[310] Z uvedeného vyplýva, že povinná osoba musí teda do 10 dní buď informácie sprístupniť, alebo vydať písomné rozhodnutie o nesprístupnení informácií. Žiadateľovi teda jednoznačne zo zákona vyplýva právo, aby sa o jeho žiadosti v zákonnej lehote (do 10 dní) rozhodlo, a to bez ohľadu na to, či vopred zaplatil finančnú úhradu materiálnych nákladov alebo nie.“[311]

Posledným princípom infozákona je princíp sprístupnenia informácií bez uvedenia dôvodu, z ktorého vyplýva, že obsahovou náležitosťou žiadosti o sprístupnenie informácie nie je vymedzenie dôvodu, pre ktorý žiadateľ žiada sprístupnenie informácie, a teda povinná osoba

[309] Pozri § 4 ods. 3 písm. c) zákona č. 145/1995 Z. z.
[310] Ide o lehotu, ktorú upravovalo vtedajšie znenie infozákona, dnes ide o lehotu ôsmich pracovných dní (pozn. autora).
[311] Rozhodnutie Krajského súdu v Bratislave sp. zn. 19 S 216/02 zo dňa 14. novembra 2002.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

nemôže ani len žiadateľa vyzvať, aby tieto dôvody uviedol. Tento princíp vyplýva z textu § 3 ods. 3 infozákona.[312]

9.4.2 Vymedzenie pojmu informácia a povinnej osoby

Jednou z významných zmien novely infozákona realizovanej prostredníctvom zákona č. 428/2022 Z. z., ktorým sa mení a dopĺňa zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov (ďalej aj ako „novela"), je aj vymedzenie pojmu informácia. Doterajšie zákonodarcovo vnímanie, podľa ktorého by definícia sa stala nástrojom reštriktívneho výkladu,[313] sa týmto krokom úplne opúšťa.

Pojem informácia tak po novom zákon vymedzuje tak pozitívne, ako aj negatívne.

Pozitívne vymedzenie pojmu informácia sa nachádza v § 4 ods. 3 infozákona. Z novely vyplýva, že za informáciu treba považovať akýkoľvek obsah v akejkoľvek forme zaznamenaný na akomkoľvek hmotnom nosiči, najmä obsah písomného záznamu v listinnej podobe, obsah písomného záznamu uloženého v elektronickej podobe alebo obsah záznamu v zvukovej, obrazovej alebo audiovizuálnej podobe. Zásadne tak tento pojem je definovaný rovnako ako je vymedzený v českom právnom poriadku,[314] ktorý bol do zákona zaradený novelou č. 61/2006 Sb., a to v súvislosti s transpozíciou smernice 2003/98 o opakovanom použití informácií verejného sektoru.[315]

Už pred novelou definoval infozákon informáciu, ale len na účely opakovaného použitia informácií. Podľa § 21b ods. 2 sa za takúto informáciu považoval akýkoľvek obsah alebo jeho časť, najmä obsah záznamu na listine, záznamu uloženého v elektronickej podobe, v podobe zvukového záznamu, zvukovo-obrazového záznamu alebo audiovizuálneho diela, v akejkoľvek forme, zaznamenané na akomkoľvek nosiči; informáciou podľa odseku 1 nie je počítačový

[312] Informácie sa sprístupňujú bez preukázania právneho alebo iného dôvodu alebo záujmu, pre ktorý sa informácia požaduje.
[313] Košičiarová, S. In Dobrovodský, R., Košičiarová, S. Právo na informácie. Krakov : Spolok Slovákov v Poľsku, 2015, s. 16.
[314] § 3 ods. 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.
[315] Furek, A., Jirovec, T. § 3. In Furek, A., Rothanzl, L., Jirovec, T. Zákon o svobodném přístupu k informacím. 1. vydání. Praha : C. H. Beck, 2016, s. 175.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

program. V právnej praxi sa však táto definícia používala aj na účely zverejňovania informácií na základe žiadosti.

Vo všeobecnosti nemožno považovať za vhodné, ak jeden pojem je na účely jedného zákona definovaný dvomi odlišnými spôsobmi, o to viac, ak tieto definície sú si mimoriadne podobné. *De lege ferenda* treba vymedziť pojem informácia len jedným spôsobom (podľa § 4 ods. 3 infozákona) a v časti upravujúcej opakované použitie informácie ponechať len špecifiká, osobitne v podobe negatívneho vymedzenia informácie (informáciou nie je počítačový program – § 21b ods. 2 infozákona).

V každom prípade však zákonodarca pozitívnou definíciou nadviazal na teoretické, ako aj judikatórne vymedzenia tohto pojmu.

P. Wilfling s odkazmi na odbornú literatúru vo vzťahu k teoretickým názorom o pojme informácia uvádza, že ide o každé oznámenie obohacujúce vedomie príjemcu alebo akýkoľvek energetický či hmotný prejav, ktorý môže mať zmysel buď pre toho, kto ho oznamuje, alebo pre toho, kto oznamované prijíma.[316] S. Košičiarová uvádza, že nedefinovaný zákonný pojem informácia znamená údaj zaznamenaný na nosič. Nie je pritom právne významné, či ide o záznam v listinnej podobe, t. j. vykonaný písomne alebo v inej technicky vykonateľnej podobe na nosiči, tzn. elektronický, zvukový, zvukovoobrazový alebo obrazový záznam.[317]

Judikatúra pri vymedzení informácie sa odvoláva na slovníkové definície tohto pojmu a uvádza, že informácia je „podľa názoru súdu správa, údaj, poučenie, ktorú fyzická osoba alebo právnická osoba odovzdáva inej fyzickej alebo právnickej osobe. Informácia je základom komunikácie. Človek ňou získava nové poznanie a komunikuje s inými ľuďmi.“[318]

„Pojem ‚informácie‘ používaný v ZSI je právnym pojmom, ktorého význam môže byť odlišný od významu používaného v bežnom hovorovom jazyku. Pri výklade tohto pojmu nachádzajúceho sa v zákone pritom treba vždy zohľadniť aj účel tohto zákona, nadväznosť

[316] Wilfling P. Zákon o slobodnom prístupe k informáciám. Komentár, problémy z praxe, rozhodnutia súdov. Pezinok : Via Iuris, 2012, s. 17.
[317] Košičiarová, S. In Dobrovodský, R., Košičiarová, S. Právo na informácie. Krakov : Spolok Slovákov v Poľsku, 2015, s. 16.
[318] Napríklad rozhodnutie Najvyššieho súdu SR sp. zn. 3Sž/16/2004 z 8. apríla 2005.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zákona na iné zákony, ústavné práva a hodnoty zakotvené v ústave a právne predpisy Európskej únie. Informáciou v zmysle ZSI je aj dokument alebo záznam, a to aj obrazový alebo zvukový a tiež aj obrazová snímka. Pri výklade pojmu ‚informácie' na účely ZSI musia súdy a orgány verejnej moci zohľadňovať skutočnosť, že zákon o slobode informácií je vykonaním ústavného práva na prístup k informáciám a že prostredníctvom neho sa realizuje ústavná povinnosť orgánov verejnej moci poskytovať informácie o svojej činnosti. Súdy a tiež orgány verejnej moci musia v zmysle čl. 152 ods. 4 Ústavy SR vykladať pojem ‚informácie' obsiahnutý v ZSI tak, aby v dôsledku tohto výkladu nebolo porušené ústavné právo verejnosti na prístup k informáciám."[319]

Časť judikatúry podporne využívala na účely definovania informácie aj vymedzenie podľa zákona o ochrane utajovaných skutočností.[320]

Zákonodarcova definícia tak potvrdzuje prístup teoretický, ako aj súdny a plne napĺňa zmysel a účel princípu čo nie je tajné, je verené.

Na druhej strane z dôvodu praktických nejasností ohľadne pozitívneho vymedzenia informácie pristúpil zákonodarca aj k negatívnemu vymedzeniu. Z dôvodovej správy vyplýva, že je to z dôvodu, aby nedochádzalo k výkladovým nejasnostiam a žiadateľ nemohol žiadať od povinnej osoby informácie, ktorých sprístupnenie by vyžadovalo administratívnu náročnosť, resp. to vyžaduje prácu navyše a povinná osoba by musela činnosťou navyše vytvárať výkladové stanoviská, rozbory, analýzy, referáty, odborné stanoviská, politické stanoviská, prognózy a výklady právnych predpisov a tiež vytvárať názory povinnej osoby.[321]

Všeobecné negatívne vymedzenie v judikatúre nenájdeme, ale na druhej strane vymedzujú sa v nej konkrétne prípady, ktoré nespadajú pod vecnú pôsobnosť infozákona ako napríklad sprístupňovanie tzv. prevádzkových informácií,[322] prípadne že informáciou nie je poskytovanie

[319] Pozri uznesenie Krajského súdu v Bratislave sp. zn. 2S 300/12-26 z 5. decembra 2012 potvrdené rozhodnutím Najvyššieho súdu SR sp. zn. 6Sži/4/2013 z 19. marca 2014.
[320] Pozri rozhodnutie Najvyššieho súdu SR sp. zn. 3 Sži 29/2013; citované podľa Ruamana, I., Šingliarová, I. (eds.) Judikatúra vo veciach slobodného prístupu k informáciám. Bratislava : Wolter Kluwer, 2014, s. 20.
[321] Dôvodová správa k novele, s. 2. Dostupné na: <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=515618>, cit. 2023-05-29.
[322] Pozri rozhodnutie Najvyššieho súdu SR sp. zn. 3 Sži 5/2013; citované podľa Rumana, I., Šingliarová, I. (eds.) Judikatúra vo veciach slobodného prístupu k informáciám. Bratislava : Wolter Kluwer, 2014, s. 15.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

obsahu spisov, prípadne informáciou podľa zákona o slobodnom prístupe k informáciám nie je (štatistické) spracovanie údajov zo stoviek spisov podľa požiadaviek, resp. pokynov toho, kto o poskytnutie informácie žiada[323] alebo odmietnutie sprístupnenia informácie ako dôsledok „zaplavenia" povinnej osoby neúmerne veľkým počtom žiadostí.[324]

Z praktických skúseností možno povedať, že negatívnym vymedzením zákonodarca reagoval na časté aplikačné problémy, keď žiadatelia žiadali o sprístupnenie informácií, ktoré boli vo svojej podstate dopytom na názor alebo určité politické rozhodnutie a podobne. Takéto informácie však povinná osoba nemala ako sprístupniť (často nemala fyzickú podobu) alebo žiadali o sprístupnenie informácií, ktoré síce povinná osoba mala, ale žiadané bolo sprístupnenie v špecifickej forme, či podobe ako napríklad v rôznych tabuľkách podľa predchádzajúceho pokynu žiadateľa ako tabuľku spracovať.

Je preto vhodné, keď zákonodarca doplnil práve toto vymedzenie do infozákona. Otázkou však ostane praktické uplatňovanie tohto vymedzenia. V každom prípade toto praktické uplatňovanie bude musieť rešpektovať súdnu judikatúru, ktorá sa zaberá problematikou vymedzenia, kedy ide o sprístupnenie informácie a kedy už o kvalitatívne spracovanie informácie do inej podoby, na ktorú sa už infozákon nevzťahuje.[325]

[323] Rozhodnutie Najvyššieho súdu SR sp. zn. 2Sžo/190/2008.
[324] Pozri rozhodnutie Ústavného súdu SR sp. zn. III. ÚS 96/2010; citované podľa Rumana, I., Šingliarová, I. (eds.) Judikatúra vo veciach slobodného prístupu k informáciám. Bratislava : Wolter Kluwer, 2014, s. 28.
[325] K tomu napríklad podľa rozhodnutia Najvyššieho súdu SR sp. zn. 6Sži/27/2013 z 24. septembra 2014: „Zo znenia zákona o informáciách nemožno vyvodzovať, že informáciou by malo byť (štatistické) spracovanie údajov zo spisov podľa požiadaviek resp. pokynov toho, kto žiada o poskytnutie informácie, taktiež z neho nevyplýva povinnosť, ktorá by povinnému subjektu ukladala získavať, vyžadovať zhromažďovať, vyhodnocovať, vyhľadávať alebo dokonca spracovať materiály žiadané žalobcom ako žiadateľom o informáciu, ak sa v ich originálnej podobe v ich dokumentácii nenachádzajú. Rovnako zo zákona o informáciách nevyplýva, že by povinné osoby museli vykonávať na žiadosť oprávnených osôb také úkony, ktoré nesmerujú k výkonu ich právomoci, alebo realizovať šetrenia, či kontrolnú alebo vyhodnocovaciu činnosť na požiadanie oprávnených osôb. Oprávnené osoby môžu požadovať len informácie o takých im neznámych skutočnostiach, ktoré má povinná osoba k dispozícii, a ktoré je povinná na žiadosť poskytnúť. Rozširujúci výklad, podľa ktorého by povinná osoba musela spracovávať údaje do inej formy, ako je tá, v ktorej sa nachádzajú, alebo poskytovať oprávnenej osobe kompletné podklady, ktoré má k dispozícii, by žiadosť o poskytnutie informácie v skutočnosti zmenil na pokyn nadriadeného, čo nebolo a nie je účelom zákona o informáciách. Žiadosť o poskytnutie informácie má za cieľ sprístupniť verejnosti jej neznáme údaje vo veciach verejných bez toho, aby sa žiadosť stala pokynom na výkon určitých činností alebo postupu povinnej osoby. Marila by sa tým výkonná aj riadiaca funkcia nadriadených, kontrolných alebo dozor vykonávajúcich orgánov a do výkonu verejnej správy by zasahovali subjekty, ktoré za jej činnosť nezodpovedajú a ani ju nevykonávajú."

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Vzhľadom na uvedené preto pod pojem informácia treba vnímať aj informácie o zamestnaneckom aparáte jednotlivých povinných osôb. Na aké subjekty preto dopadá táto informačná povinnosť? Ich vymedzenie sa nachádza v § 2 infozákona.

Prvú skupinu povinných osôb tvoria štátne orgány, obce, vyššie územné celky ako aj tie právnické osoby a fyzické osoby, ktorým zákon zveruje právomoc rozhodovať o právach a povinnostiach fyzických osôb alebo právnických osôb v oblasti verejnej správy, a to iba v rozsahu tejto ich rozhodovacej činnosti.

V tejto skupine povinných osôb sa teda nachádzajú v prvom rade orgány verejnej moci a v druhom rade osoby súkromného práva (fyzické alebo právnické), ktorým osobitné zákony priznali právo rozhodovať o právach a povinnostiach fyzických osôb alebo právnických osôb. Z literatúry sa dozvedáme, že ide napríklad o členov stráží alebo stanice technickej kontroly. Tieto súkromné osoby majú obmedzenú informačnú povinnosť, pretože informujú iba o svojej rozhodovacej činnosti.

Druhú skupinu povinných osôb tvoria právnické osoby zriadené zákonom a právnické osoby zriadené štátnym orgánom, vyšším územným celkom alebo obcou podľa osobitného zákona. V tomto prípade ide o rozličné právnické osoby verejného práva a tiež o osoby, ktoré sú príspevkovými alebo rozpočtovými organizáciami štátu, obcí alebo samosprávnych krajov.

Napokon tretiu skupinu tvoria zdravotné poisťovne a ďalej aj právnické osoby, ak v nich povinné osoby prvej a druhej skupiny majú samostatne alebo spoločne aspoň väčšinovú priamu alebo nepriamu účasť, a ak súčasne

a) sú kontrolované povinnou osobou prvej alebo druhej skupiny, alebo

b) povinná osoba prvej alebo druhej skupiny priamo alebo nepriamo navrhuje alebo ustanovuje viac ako polovicu členov ich riadiaceho orgánu alebo kontrolného orgánu.

Pokiaľ ide o skupinu osôb, kde štát, samospráva a ďalšie verejné subjekty majú účasť, tak V zmysle dikcie novej právnej úpravy teda bude pre vznik informačnej povinnosti takejto právnickej osoby rozhodujúci vplyv verejnej zložky (t. j. štátu, samospráv a ich inštitúcií) na právnickú osobu. Za účelom vylúčenia vzniku informačnej povinnosti pre akýkoľvek typ

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

právnických osôb, v ktorých bude mať čo i len marginálnu participáciu verejný prvok bol zákonodarcom stanovený princíp väčšinovej účasti verejného prvku v právnickej osobe a kumulatívne splnenie podmienky kontroly alebo ustanovenia väčšiny členov riadiaceho, resp. kontrolného orgánu zo strany povinnej osoby podľa § 2 ods. 1 alebo 2 zákona o slobode informácií. Pod pojmom priama alebo nepriama účasť je potrebné mať na zreteli výkon práv vo vzťahu k spoločnosti (najmä výkon riadiacich oprávnení a tiež majetkové zdieľanie výsledkov činnosti obchodnej spoločnosti), a to bez sprostredkovateľa (priamo) ale-bo prostredníctvom tretej osoby (nepriamo). Za nepriamu účasť zákonodarca považuje práve vertikálnu rovinu majetkových vzťahov.[326]

9.4.3 Ochrana osobných údajov v infozákone

Predmetná výnimka z princípu čo nie je tajné, je verejné, je ustanovenie § 9 infozákona, ktorý v 4 odsekoch vymedzuje výnimky z dôvodu uplatnenia ochrany osobnosti a osobných údajov. Ochrana osobnosti je predmetom odseku 1 a ochrana osobných údajov predmetom nasledujúcich 3 odsekov (t. j. odseky 2 až 4).

Všeobecne k danému ustanoveniu Najvyšší súd SR uviedol, že „Účelom ustanovenia § 9 zák. č. 211/2000 Z. z. je chrániť informácie týkajúce sa súkromia a osobné údaje fyzických osôb. Právo na ochranu súkromia je právo osoby rozhodnúť podľa vlastného uváženia, či, v akom rozsahu a akým spôsobom majú byť skutočnosti jej osobného súkromia sprístupnené iným. Súčasťou práva na ochranu súkromia je aj ochrana osobných údajov. Právo na súkromie však zahŕňa aj právo na ochranu informácií a skutočností, ktoré sa celkom nedajú kvalifikovať ako osobné údaje. Ide napríklad o písomnosti osobnej povahy, podobizne, obrazové snímky a obrazové a zvukové záznamy týkajúce sa fyzickej osoby alebo jej prejavov osobnej povahy. Právo na ochranu súkromia a prejavov osobnej povahy je tiež aj súčasťou práva na ochranu osobnosti podľa § 11 Občianskeho zákonníka.“[327]

Podľa § 9 ods. 2 až 4 infozákona:

[326] Ivančík, J. Rozšírenie okruhu povinných osôb v oblasti práva na informácie po legislatívnych zmenách v roku 2022. In Acta Facultatis Iuridicae Universitatis Comenianae, Vol. 42, č. 1 (2023), s. 59-60.
[327] Rozsudok Najvyššieho súdu SR sp. zn. 6 Sžo 250/2008 z 25. novembra 2009.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

(2) Informácie o osobných údajoch fyzickej osoby, ktoré sú spracúvané v informačnom systéme za podmienok ustanovených osobitným zákonom, povinná osoba sprístupní len vtedy, ak to ustanovuje zákon, alebo na základe predchádzajúceho písomného súhlasu dotknutej osoby. Ak dotknutá osoba nemá spôsobilosť na právne úkony, taký súhlas môže poskytnúť jej zákonný zástupca. Ak dotknutá osoba nežije, taký súhlas môže poskytnúť jej blízka osoba; súhlas sa nevyžaduje, ak ide o sprístupňovanie osobných údajov zosnulej dotknutej osoby na vedecký účel, na štatistický účel, na účel archivácie, dokumentačnej činnosti, historického výskumu, činností pohrebísk, umiestnenia pamätníkov a pamätných tabúľ, konania spomienkových podujatí a piety v rozsahu nevyhnutnom pre jeho naplnenie.

(3) Povinná osoba sprístupní na účely informovania verejnosti osobné údaje fyzickej osoby, ktoré sú spracúvané v informačnom systéme za podmienok ustanovených osobitným zákonom o fyzickej osobe, ktorá je verejným funkcionárom, poslancom obecného zastupiteľstva, predstaveným v štátnej službe, odborníkom plniacim úlohy pre člena vlády Slovenskej republiky, prezidenta Slovenskej republiky, predsedu Národnej rady Slovenskej republiky alebo podpredsedu Národnej rady Slovenskej republiky, vedúcim zamestnancom vykonávajúcim práce vo verejnom záujme, vedúcim zamestnancom zamestnávateľa, ktorým je orgán verejnej moci, nadriadeným v služobnom pomere alebo členom hodnotiacej komisie alebo iného obdobného orgánu, ktorý sa zúčastňuje na procese rozhodovania o použití verejných prostriedkov. Podľa prvej vety sa sprístupňujú osobné údaje v rozsahu

a) titul,
b) meno,
c) priezvisko,
d) funkcia a deň ustanovenia alebo vymenovania do funkcie,
e) pracovné zaradenie a deň začiatku výkonu pracovnej činnosti,
f) miesto výkonu funkcie alebo pracovnej činnosti a orgán, v ktorom túto funkciu alebo činnosť vykonáva,

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

g) mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, ak sú uhrádzané zo štátneho rozpočtu alebo z iného verejného rozpočtu.

(4) Osobné údaje osoby, ktorá je nadriadeným v služobnom pomere, povinná osoba sprístupní v rozsahu a na účel podľa odseku 3, len ak sprístupnenie nie je v rozpore s povinnosťou mlčanlivosti podľa osobitných predpisov a zároveň sprístupnenie tejto informácie neohrozí bezpečnosť alebo obranu Slovenskej republiky, ochranu verejného poriadku alebo plnenie úloh týchto osôb alebo orgánov, v ktorých vykonávajú svoju činnosť; ustanovenie § 13 sa v tomto prípade nepoužije.

Odsek 2 predmetného ustanovenia chráni osobné údaje zamestnancov povinných osôb pred ich sprístupnením verejnosti. Možnosti ich sprístupnenia sú dve, a to vtedy ak tak určí osobitný právny predpis (môže ísť napríklad o zamestnancov, ktorí sú členmi určitých poradných, iniciatívnych a iných orgánov, a preto osobitný predpis v záujme transparentnosti vyžaduje zverejnenie ich totožnosti), alebo vtedy, ak dá súhlas na zverejnenie priamo tá osoba, ktorej sa tieto osobné údaje týkajú. Povinná osoba nie je podľa zákona povinná tento súhlas aktívne získavať; tento súhlas však môže získavať, ale je to na jej zvážení. Povinnosť získania súhlasu rovnako tak dopadá aj na žiadateľa.

To podporuje aj súdna judikatúra, podľa ktorej: „ak žiadateľ požiada o sprístupnenie informácií o súkromí alebo osobných údajov (resp. dokumentov obsahujúcich tieto informácie), povinná osoba ich podľa § 9 ods. 1 a 2 zák. č. 211/2000 Z. z. sprístupní len vtedy, ak to ustanovuje osobitný zákon alebo na základe predchádzajúceho písomného súhlasu dotknutej osoby (osoby, ktorej sa týka informácia o súkromí alebo osobný údaj). Keďže tieto ustanovenia neukladajú povinnej osobe povinnosť požiadať o písomný súhlas dotknutej osoby, povinná osoba nemusí žiadať dotknutú osobu (resp. blízku osobu alebo zákonného zástupcu) o súhlas. Ak žiadateľ o informáciu nevie preukázať takýto súhlas dotknutej osoby alebo ak súhlas nie je založený v úradnom spise, povinná osoba informáciu nesprístupní.“[328]

[328] Rozsudok Najvyššieho súdu SR sp. zn. 6 Sžo 250/2008 z 25. novembra 2009.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Odsek 3 a 4 upravujú tzv. princíp prevažujúceho verejného záujmu,[329] ako výnimku z nesprístupňovania určitých informácií týkajúcich sa verejných funkcionárov verejnosti. Táto výnimka sa netýka všetkých zamestnancov povinných osôb, ale len tých, ktorí sú vymedzený v odseku 3. V zásade ide o verejných funkcionárov, alebo vedúcich zamestnancov.

Pri týchto osobách existuje verejný záujem na tom, aby mala verejnosť informácie o ich činnosti. Sprístupnenie týchto informácií nie je porušením ochrany osobných údajov alebo súkromia. Ide o vyjadrenie princípu prevažujúceho verejného záujmu. Formulácia „mzda, plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti“ zahŕňa okrem mzdy a platu aj napríklad odmeny, funkčné príplatky, cestovné náhrady alebo tzv. paušálne náhrady.[330]

Toto ustanovenie si pritom prešlo aj testom ústavnosti a Ústavný súd SR ho tak vyhlásil za súladný s ústavným poriadkom Slovenskej republiky. Podľa tohto súdu: „Podľa ústavného súdu sa právo na informácie nepochybne vzťahuje na informácie týkajúce sa nakladania s verejnými prostriedkami, ktorému nemožno uprieť aj charakter politickej otázky. Prístup širokej verejnosti k týmto informáciám vytvára priestor na verejnú kontrolu hospodárenia všetkých subjektov, ktorých príjmy sú vyplácané z verejných rozpočtov, a to tak vo vzťahu k ich zákonnosti, ako aj účelnosti. Možno poznamenať, že sa do tohto prístupu premieta demokratický charakter štátu. Súčasťou otázky nakladania s verejnými prostriedkami sú pritom aj príjmy verejných činiteľov alebo iných osôb, ktoré pochádzajú z verejných rozpočtov. Pokiaľ ide o tieto príjmy, treba však rozlišovať medzi platmi, ktorých výšku možno vyvodiť priamo zo zákona, a odmenami, o ktorých rozhodujú verejní funkcionári. Napadnuté ustanovenie sa preto v podstate dotýka len odmien, ktorých priznávanie vytvára potenciálnu možnosť korumpovania vysokých štátnych úradníkov, resp. špecifickú formu zabezpečenia ich lojality, ako aj možnosť, aby verejní funkcionári, ktorí o výške odmien rozhodujú, zneužívali svoje postavenie a právomoci.

Ako už bolo uvedené, ústavný súd nemá pochybnosti o citlivosti údajov o výške príjmov pre súkromnú sféru jednotlivca, ako aj o tom, že jej zverejnenie môže mať pre túto jeho sféru

[329] Wilfling, P. Zákon o slobodnom prístupe k informáciám. Komentár. Pezinok : Via Iuris, 2012, s. 86.
[330] Tamtiež.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

negatívne dôsledky. V prípade dotknutých osôb však ide len o jeden aspekt, ktorý je z hľadiska vlastného posúdenia veci potrebné vziať do úvahy. Ďalším aspektom je totiž práve verejný záujem na verejnej kontrole a transparentnosti nakladania s verejnými prostriedkami z hľadiska jeho zákonnosti a účelnosti, ako aj preventívne pôsobenie takejto kontroly. Z tohto aspektu je nevyhnutné zdôrazniť, že základné právo na informácie slúži vo svojej podstate aj ako prekážka pre zneužívanie moci zo strany osôb podieľajúcich sa na jej výkone. Účinná kontrola verejnej moci tak nie je skutočná (efektívna) bez možnosti prijímať informácie vzťahujúce sa na jednotlivé osoby, ktoré túto moc vykonávajú. Verejný záujem na informáciách o príjmoch jednotlivých osôb uvedených v § 9 ods. 3 prvej vete zákona č. 211/2000 Z. z. pritom reflektuje aj skutočnosť, že informácia o pravidelných i nepravidelných (mimoriadnych) príjmoch môže mať výpovednú hodnotu z hľadiska faktického postavenia a účasti týchto osôb na prijímaní rozhodnutí orgánov verejnej moci, a to politického aj nepolitického charakteru. Túto skutočnosť treba zvlášť zdôrazniť s ohľadom na spoločenskú realitu, keď významná časť nielen vedúcich miest v štátnych inštitúciách, resp. inštitúciách financovaných z verejných rozpočtov je obsadzovaná reflektujúc aktuálne politické pomery.

Z hľadiska rozhodovania ústavného súdu bol ďalej významný už zmienený záver, že osoby podieľajúce sa na výkone verejnej moci musia počítať s vyššou mierou obmedzenia ich základného práva na súkromie. V danom prípade je pritom významné aj to, že platové pomery vo verejnej správe sú určované príslušnou právnou úpravou a ich ďalšie pravidelné alebo nepravidelné zložky sú, čo sa týka výšky, touto úpravou významne limitované. To, samozrejme, nemožno stotožňovať s individualizáciou výšky príjmu, ku ktorej dochádza vo vzťahu k jednotlivým fyzickým osobám uvedeným v § 9 ods. 3 prvej vete zákona č. 211/2000 Z. z. na základe napadnutého ustanovenia. Táto skutočnosť však poukazuje na to, že výška príjmov pochádzajúcich z verejných rozpočtov presahuje ich súkromnoprávny charakter a je spôsobilá byť otázkou verejného záujmu, resp. verejnej diskusie. Napokon ústavný súd s ohľadom na výpočet osôb uvedených v napadnutom ustanovení zdôraznil, že povinnosť poskytnúť informácie sa nevzťahuje na všetky osoby, ktoré poberajú plat z verejných rozpočtov, ale len na taxatívne vymenovaných verejných funkcionárov ustanovených zákonom (vysokých štátnych úradníkov), ktorí sú buď riadiacimi pracovníkmi, alebo majú špecifické postavenie

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

odôvodňujúce väčšiu intenzitu zásahu do svojho práva na súkromie. Posúdenie proporcionality v danom prípade sa tak týka len zverejnenia údajov vo vzťahu k týmto osobám, a nie všetkým zamestnancom štátu.

Ústavný súd nesúhlasí s názorom navrhovateľa „o ničím neodôvodnenom tvrdení o nadradenosti politického práva na informácie nad základným ľudským právom na ochranu osobných údajov" u skupiny osôb uvedenej v napadnutom ustanovení. Naopak, musí poukázať na skutočnosť, že navrhovateľ vo svojej argumentácii nijakým relevantným spôsobom nerozviedol svoje tvrdenie o tom, prečo z hľadiska vzájomného vyvažovania v kolízii stojacich hodnôt má mať väčšiu váhu práve právo na ochranu osobných údajov. S ohľadom na túto argumentáciu je zrejmé, že ústavný súd sa nestotožnil s pochybnosťami navrhovateľa, a teda že dospel k záveru, že napadnuté ustanovenie je v súlade s čl. 19 ods. 3 a čl. 22 ods. 1 ústavy. Vychádzajúc z uskutočneného testu proporcionality pritom dospel k rovnakému záveru aj vo vzťahu k čl. 1 ods. 1 a čl. 13 ods. 2, 3 a 4 ústavy."[331]

Zároveň platí, že informácie podľa odseku 3 sprístupňuje povinná osoba v zásade len na základe žiadosti, a nie proaktívne. V právnej praxi súdy posudzovali prípad, keď obecné zastupiteľstvo svojím uznesením uložilo obecnému úradu zverejniť vždy k 30. dňu nasledujúceho mesiaca po mesiaci odpracovanom plat alebo platové pomery a ďalšie finančné náležitosti priznané za výkon funkcie alebo za výkon pracovnej činnosti, uhrádzané z verejného rozpočtu vedúcim zamestnancom vykonávajúcim práce vo verejnom záujme, vedúcim zamestnancom zamestnávateľa, ktorým je orgán verejnej moci. Išlo o obecný úrad či o obcou zriadené rozpočtové organizácie. Súdy tento výklad infozákona odmietli.

V tomto prípade: „Súd preskúmal napadnuté uznesenie obecného zastupiteľstva Obce XXX a na základe vykonaného dokazovania dospel k záveru, že toto nie je v súlade s platnou právnou úpravou. V danom prípade súd zhodne ako navrhovateľ konštatuje, že prijatím tohto uznesenia došlo k porušeniu právomoci a pôsobnosti obecného zastupiteľstva primárne stanovenej v § 11 ods. 4 zákona o obecnom zriadení. Z citovaného zákonného ustanovenia nevyplýva, žeby obecné zastupiteľstvo mohlo vykonávať pôsobnosť nadriadeného subjektu s

[331] Nález Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 1/09 z 19. januára 2011.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

rozhodovacou právomocou voči obecnému úradu a jeho aparatúre. Môže vykonávať len tie úlohy, ktoré mu zveruje zákon. Z úvodnej vety § 11 ods. 4 zákona o obecnom zriadení vyplýva, že obecné zastupiteľstvo rozhoduje o základných otázkach života obce, i preto je možné mať za to, že zverejnenie mzdy, platu alebo platových pomerov a ďalších finančných záležitostí v rozsahu uvedenom v cit. uznesení je skôr inou záležitosťou než otázkou rozhodne dôležitou pre život v obci, o ktorej by prináležalo rozhodovať zastupiteľstvu. Ak teda orgán územnej samosprávy opatrením uloží novú povinnosť, ktorá neexistuje v zákone, resp. ktorú nemožno zo zákona odvodiť, uplatňuje svoju normotvornú právomoc spôsobom, ktorý nie je v súlade s čl. 2 ods. 3 Ústavy SR.

Toto uznesenie zároveň nerešpektuje ani zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám, keďže obecnému úradu a jeho aparatúre uložilo povinnosť zverejňovať pravidelne v určenom čase informáciu v zmysle § 9 ods. 3 citovaného zákona, ktorú síce má obec ako jeden z povinných subjektov uvedených v § 2 ods. 1, 2 a 3 zákona o slobodnom prístupe k informáciám, avšak tomuto sprístupneniu musí predchádzať žiadosť žiadateľa, pretože v danom prípade nejde o povinné zverejňovanie informácií v zmysle § 5, 5a, 5b a 6 zákona o slobodnom prístupe k informáciám.“[332]

9.4.4 Závery

Právo na ochranu osobných údajov tak majú aj zamestnanci orgánov verejnej moci, ktoré sú inak v pozícii tzv. povinných osôb podľa infozákona. Platí tu, že pokiaľ povinná osoba sprístupňuje informácie, musí ich sprístupniť tak, aby zároveň chránila osobné údaje v týchto informáciách uvedené. Štandardne sa to robí postupom, keď sa tieto údaje tzv. začiernia (§ 12 infozákona). Inak sa osobné údaje sprístupnia len v takom prípade, ak tak ustanovuje osobitný zákon alebo ak s tým priamo dotknutá osoba súhlasí. Povinná osoba (orgán verejnej moci) však nie je povinný takýto súhlas aktívne získavať.

Z dôvodu aplikácie princípu prevažujúceho verejného záujmu, v prípade taxatívne vymedzených osôb pôsobiacich na orgánoch verejnej moci, sa určité osobné údaje sprístupňujú verejnosti na základe žiadosti. Ide najmä o osoby, ktoré sú vedúcimi týchto

[332] Rozsudok Krajského súdu v Košiciach sp. zn. 7S/52/2014 zo 14. januára 2015.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

orgánov alebo vedúcimi zamestnancami, čiže čiastočný zásad ho ich práva na ochranu súkromia je tu nevyhnutný s cieľom zabezpečenia verejnej kontroly. Zákon potom presne vymedzuje, ktoré údaje možno v ich prípade sprístupniť. Zároveň platí, že tieto informácie sa nesprístupňujú aktívnym spôsobom, ale výlučne na základe žiadosti.

9.5 AUTOMATIZOVANÉ ROZHODOVACIE SYSTÉMY

Digitalizácia ovplyvňuje svet práce a riadenie ľudských zdrojov. Automatizované rozhodovacie systémy (algoritmické riadenie, algoritmický manažment) sa stávajú čoraz viac rozšírenými a slúžia na prijímanie rozhodnutí, ktoré boli pôvodne vyhradené človeku.

Používajú sa vo všetkých fázach pracovného života a významne ovplyvňujú pracovné podmienky a postavenie zamestnancov. Od vstupu do zamestnania na kontrolu a vyhodnocovanie žiadostí a životopisov, výber koho pozvať na pohovor a s kým založiť pracovný pomer. Cez jeho trvanie na prideľovanie úloh, monitorovanie, dozor, hodnotenie pracovného výkonu, odmeňovanie, predpovedanie budúceho správania, či disciplinárne opatrenia, ktoré môžu viesť až k prepúšťaniu. Je teda zrejmé, že pre zamestnancov predstavujú riziká pokiaľ ide o realizáciu základných slobôd, ako právo na prácu, ochranu zdravia, dôstojnosti a súkromia.

So zavádzaním rozhodovacích nástrojov umelej inteligencie na pracoviskách sú spojené praktické otázniky, ktoré zasahuje do pôsobnosti viacerých oblastí, včítane rýdzeho pracovného práva reprezentovaného Zákonníkom práce č. 311/2001 Z.z., zásady rovného zaobchádzania, bezpečnosti pri práci a osobných údajov. Je tu však otázka, do akej miery postačujú existujúci legislatívny rámec, najmä ak v ňom chýba výslovná úprava algoritmického riadenia.

9.5.1 Osobitná úprava v GDPR

Vzhľadom na masívny tok spracúvaných dát pri rozhodnutiach, ktoré sú prijímané automatizovanými systémami, sa práva patriace zamestnancom čiastočne prekrývajú so zárukami vyplývajúcimi z nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (GDPR).

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Všeobecné nariadenie sa v plnom rozsahu vzťahuje aj na automatizované rozhodovacie systémy. Popri univerzálnych podmienkach (právo na informácie, prístup k údajom + posúdenie vplyvu na ochranu údajov) obsahuje aj jedno špeciálne pravidlo.

Článok 22 označený ako Automatizované *individuálne rozhodovanie vrátane profilovania* sa na jednej strane považuje za najdôležitejšiu poistku pred ujmou spôsobenou algoritmickým riadením. Na strane druhej však ide o najviac zložité a kontroverzné ustanovenie v teórii i praxi.[333]

Vychádza zo základnej premisy, že vysokorizikové rozhodnutia by mal prijímať človek a nie algoritmy:

a) Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.

b) Odsek 1 sa neuplatňuje, ak je rozhodnutie:

   a. nevyhnutné na uzavretie alebo plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom,

   b. povolené právom Únie alebo právom členského štátu, ktorému prevádzkovateľ podlieha a ktorým sa zároveň stanovujú aj vhodné opatrenia zaručujúce ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, alebo

   c. založené na výslovnom súhlase dotknutej osoby.

c) V prípadoch uvedených v odseku 2 písm. a) a c) prevádzkovateľ vykoná vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, a to aspoň práva na ľudský zásah zo strany prevádzkovateľa, práva vyjadriť svoje stanovisko a práva napadnúť rozhodnutie.

[333] ABRAHA, H. Regulating algorithmic employment decisions through data protection law. S. 9

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

d) Rozhodnutia uvedené v odseku 2 sa nezakladajú na osobitných kategóriách osobných údajov uvedených v článku 9 ods. 1, pokiaľ sa neuplatňuje článok 9 ods. 2 písm. a) alebo g) a nie sú zavedené vhodné opatrenia na zaručenie práv a slobôd a oprávnených záujmov dotknutej osoby.

Pozri aj odôvodnenie 71 GDPR: „Dotknutá osoba by mala mať právo nepodliehať rozhodnutiu, ktoré môže zahŕňať opatrenie, hodnotiacemu osobné aspekty, ktoré sa jej týkajú, založenému výlučne na automatizovanom spracúvaní a ktoré má právne účinky, ktoré sa dotknutej osoby týkajú alebo ju podobným spôsobom významne ovplyvňujú, ako je napríklad automatické zamietnutie online žiadosti o úver alebo elektronické postupy prijímania pracovníkov bez akéhokoľvek ľudského zásahu. Takéto spracúvanie zahŕňa 'profilovanie' pozostávajúce z akejkoľvek formy automatizovaného spracúvania osobných údajov spočívajúceho v hodnotení osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým na analýzu alebo predvídanie aspektov súvisiacich s výkonnosťou dotknutej osoby v práci, jej majetkovými pomermi, zdravím, osobnými preferenciami alebo záujmami, spoľahlivosťou alebo správaním, polohou alebo pohybom, pokiaľ vedie k právnym účinkom, ktoré sa dotknutej osoby týkajú alebo ju podobným spôsobom významne ovplyvňujú.“

Vysokorizikovosť vyplýva z odôvodnením 36 návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii): *„Ako* vysokorizikové *by sa mali klasifikovať aj systémy umelej inteligencie používané pri zamestnávaní, riadení pracovníkov a prístupe k samostatnej zárobkovej činnosti, najmä pri nábore a výbere osôb, pri rozhodovaní o povýšení a ukončení pracovného pomeru a pri prideľovaní úloh, monitorovaní alebo hodnotení osôb v zmluvných pracovnoprávnych vzťahoch, pretože tieto systémy môžu významne ovplyvniť budúce kariérne vyhliadky a živobytie týchto osôb. Príslušné zmluvné pracovnoprávne vzťahy by mali zahŕňať zamestnancov a osoby, ktorí poskytujú služby prostredníctvom platforiem, ako sa uvádza v pracovnom programe Komisie na rok 2021. Takéto osoby by sa v zásade nemali považovať za používateľov v zmysle tohto nariadenia. Takéto systémy môžu počas celého procesu prijímania do zamestnania a počas hodnotenia, povyšovania alebo udržiavania osôb v zmluvných pracovnoprávnych vzťahoch zachovávať zaužívané formy diskriminácie, napríklad žien,*

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

určitých vekových skupín, osôb so zdravotným postihnutím alebo osôb určitého rasového alebo etnického pôvodu alebo sexuálnej orientácie. Systémy umelej inteligencie používané na monitorovanie výkonnosti a správania týchto osôb môžu mať vplyv aj na ich práva na ochranu údajov a súkromia."

Rovnako bod 4 prílohy III aktu o umelej inteligencii, ktorý explicitne uvádza zoznam vysokorizikových systémov umelej inteligencie: „*Zamestnanosť, riadenie pracovníkov a prístup k samostatnej zárobkovej činnosti:*

a) systémy umelej inteligencie určené na nábor alebo výber fyzických osôb, najmä na inzerovanie voľných pracovných miest, preverovanie alebo filtrovanie žiadostí, hodnotenie uchádzačov počas pohovorov alebo skúšok;

b) systémy umelej inteligencie, ktoré sa majú používať pri rozhodovaní o postupe v zamestnaní a ukončení zmluvných pracovných vzťahov, pri prideľovaní úloh a monitorovaní a hodnotení výkonnosti a správania osôb v rámci takýchto vzťahov."

9.5.2 Výlučne automatizované spracovanie

Zásadným problémom, od ktorého s odvíja celá aplikácia, je formulácia, že zamestnanec nesmie byť predmetom rozhodnutia založenom výhradne na automatizovanom spracovaní osobných údajov. Na prvý pohľad sa teda javí, že v rozhodovacom procese nesmie vôbec figurovať človek. Nie je však také jednoznačné.

Častica výlučne reálne znamená, že zahrnuté by mali byť aj systémy, v ktorých je prítomný ľudský prvok. Pracovná skupina pre ochranu údajov zriadená podľa Článku 29 (v súčasnosti premenovaná na Európsky výbor pre ochranu údajov - EDPB) vo svojich inštrukciách už objasnila, že *„[p]revádzkovateľ nemôže obísť ustanovenia článku 22 tým, že vytvorí ľudskú účasť. Napríklad, ak* niekto *bežne uplatňuje automaticky generované profily na jednotlivcov bez akéhokoľvek skutočného vplyvu na výsledok, stále by to bolo rozhodnutie založené výlučne na automatizovanom spracúvaní. Aby sa to mohlo kvalifikovať ako ľudská účasť, prevádzkovateľ musí zabezpečiť, aby akýkoľvek dohľad nad rozhodnutím bol zmysluplný, a nebolo to len symbolické gesto. Mal by ho vykonávať niekto, kto má právomoc a kompetenciu*

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zmeniť rozhodnutie. Ako súčasť analýzy by mal zvážiť všetky relevantné údaje“[334]. Inými slovami, ľudská validácia *pro forma* (v tech žargóne známa ako *rubber-stamping*[335]) nesmie slúžiť na popretie skutočnosti, že rozhodnutie spadá pod pôsobnosť automatizovaného rozhodovacieho systému.

Samozrejme, tu hneď vyvstávajú otázky, čo si predstaviť pod zmysluplným ľudským vkladom, či v ktorej fáze rozhodovacieho procesu sa vyžaduje zapojenie človeka. Stručne možno uviesť, že konajúca osoba by mala byť schopná nezávisle posúdiť prípad a zhodnotiť výstupy systému, a nie ich iba odkývať bez rozmyslu. Mala by mať oprávnenie zrušiť automatizované výstupy a zvažovať dodatočné informácie a poľahčujúce faktory.[336]

9.5.2.1 Právo alebo zákaz?

Zainteresovaným stranám nepomáha ani nejednoznačná textácia odsek 1.: či ide o absolútny zákaz automatizovaného rozhodovania, alebo o právo dotknutej osoby namietať ho? Každá z interpretácií má rozdielne dopady nielen na subjekty pracovnoprávnych vzťahov, ale aj na postup úradu na ochranu osobných údajov.

Podľa EDPB, „[p]ojem 'právo' v tomto ustanovení neznamená, že článok 22 ods. 1 sa uplatňuje iba vtedy, keď sa naň dotknutá osoba aktívne odvoláva. V článku 22 ods. 1 sa stanovuje všeobecný zákaz rozhodovania založeného výlučne na automatizovanom spracúvaní. Tento zákaz sa uplatňuje bez ohľadu na to, či dotknutá osoba podniká kroky týkajúce sa spracúvania svojich osobných údajov.“ (...) Tento výklad posilňuje myšlienku, že dotknutá osoba má kontrolu nad svojimi osobnými údajmi, čo je v súlade so základnými zásadami GDPR. Výklad článku 22 ako zákaz, a nie právo, ktoré sa má uplatniť, znamená, že jednotlivci sú automaticky

[334] Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679 Prijaté 03.10.2017, naposledy revidované a prijaté 06.02.2018, s. 20
[335] ALOISI, A. – POTOCKA-SIONEK, N.: De-gigging the labour market? An analysis of the ‘algorithmic management’ provisions in the proposed Platform Work Directive, Italian Labour Law e-Journal Issue 1, Vol. 15 (2022) s. 39
[336] Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR Reuben Binns - Michael Veale, s. 320 International Data Privacy Law, 2021, Vol. 11, No. 4

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

chránení pred potenciálnymi účinkami, ktoré môže mať tento typ spracúvania. (...) To znamená, že spracúvanie podľa článku 22 ods. 1 nie je všeobecne povolené.[337]

Uvedený názor je akceptovaný väčšinou odbornej literatúry, rátajúc do toho všetky zdroje využité v tomto článku. Mne dáva tiež význam, pretože poskytuje lepšiu ochranu záujmov zamestnancov.

Za pozornosť však stojí predovšetkým protiargumentácia Tosoniho, ktorý je v zmysle jazykového, kontextového, systematického a teleologického výkladu presvedčený, že GDPR v skutočnosti dáva dotknutým osobám právo, ktoré môžu vykonávať podľa vlastného uváženia. Súčasne si však uvedomuje, že bude ťažké získať podporu stakeholderov pre svoje tvrdenia, pretože sú v rozpore s vyššie citovaným metodickým usmernením.[338]

9.5.2.2 Výnimky

Okrem toho, že článok 22 je napísaný pomerne vágne, tak podlieha aj viacerým výnimkám, ktoré môžu pozitívny efekt pre zamestnanca spraviť bezzubým. Absolútny zákaz je relativizovaný. Zamestnávateľ by nemal vykonávať automatizované rozhodovanie, pokiaľ sa neuplatňuje aspoň niektorá z troch výnimiek podľa odseku 2.

9.5.2.3 Nevyhnutnosť uzavretia alebo plnenia zmluvy

V súvislosti s výkonom závislej práce je obzvlášť relevantný právny základ (pred)zmluvnej nevyhnutnosti, ak neexistujú iné účinné a menej rušivé prostriedky na dosiahnutie toho istého cieľa.

EDPB uvádza ako modelový príklad situáciu, kedy rutinné ľudské zapojenie môže byť nepraktické alebo nemožné z dôvodu množstva spracúvaných údajov: „*Podnik inzeruje voľné pracovné miesto. Keďže práca pre predmetný podnik je populárna, podnik dostáva desiatky tisíc žiadostí. V dôsledku mimoriadne vysokého objemu žiadostí môže podnik zistiť, že prakticky nie je možné identifikovať vhodných kandidátov bez toho, aby sa najprv použili plne*

[337] Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, s. 19.
[338] TOSONI, L. The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation, International Data Privacy Law, 2021, Vol. 11, No. 2 145-162

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

automatizované prostriedky na vyradenie irelevantných žiadostí. V tomto prípade môže byť potrebné automatizované rozhodovanie, aby sa vytvoril užší zoznam možných kandidátov, s úmyslom uzavrieť zmluvu s dotknutou osobou."[339]

Naproti tomu jedna z nemeckých agentúr na ochranu osobných údajov *Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg* zaujala opačný postoj. Vo svojej výročnej správe uviedla, že automatizované jazykové analýzy písomných prejavov (CV, motivačný list) uchádzačov o zamestnanie, ktoré rozhodujú s kým pokračovať vo výberovom konaní, sa môžu vykonávať len s ich predchádzajúcim súhlasom. Vzápätí však dodala, že dobrovoľný charakter súhlasu je viac ako otázny, pretože namieste sú obavy kandidátov, že ak súhlas neposkytnú, nebude sa nich ďalej prihliadať.[340]

9.5.2.4 Súhlas

Ide teda o výnimku, ktorá vzbudzuje pochybnosť o dostatočnej ochrane slabšej zmluvnej strany. Napriek tomu, že nestačí súhlas 'obyčajný', ale vyžaduje sa výslovný, ide o pomerne jednoduchý spôsob obídenia zákazu nasadzovania automatizovaných rozhodovacích systémov, keďže pre zamestnávateľa nie je ťažké, hoc aj explicitný, súhlas získať. Derogáciu únijný normotvorca zakotvil napriek tomu, že - so zreteľom na povahu pracovnoprávneho vzťahu - zamestnanec spravidla nie je v pozícií, aby mohol súhlas slobodne vyjadriť, odmietnuť jeho udelenie alebo odvolať.

Okrem toho výslovný súhlas nie je vhodný tiež preto, že „algoritmy sú zo svojej podstaty netransparentné z hľadiska ich funkcie a dizajnu alebo preto, že aj keď sú transparentné, tak nemusia byť pre dotknutú osobu zrozumiteľné"[341].

9.5.2.5 Povolenie právom

[339] Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, s. 23.
[340] Tätigkeitsbericht Datenschutz 2020, s. 106, dostupné na https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/02/LfDI-BW_36_Ta%CC%88tigkeitsbericht_2020_WEB.pdf
[341] Kamarinou, Dimitra and Millard, Christopher and Singh, Jatinder, Machine Learning with Personal Data (November 7, 2016). Queen Mary School of Law Legal Studies Research Paper No. 247/2016, s. 15

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

GDPR ďalej umožňuje na vnútroštátnej úrovni odkloniť sa od zákazu zavedením špecifického prijatím osobitnej úpravy. Slovenská republika, rovnako ako väčšina členských štátov, túto možnosť nevyužila a v podstate iba skopírovala Článok 22:

[1] „Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní osobných údajov vrátane profilovania a ktoré má právne účinky, ktoré sa jej týkajú alebo ju obdobne významne ovplyvňujú.

[2] Odsek 1 sa neuplatňuje, ak je rozhodnutie

a) nevyhnutné na uzavretie zmluvy alebo plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom,

b) vykonané na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, a v ktorých sú zároveň ustanovené aj vhodné opatrenia zaručujúce ochranu práv a oprávnených záujmov dotknutej osoby, alebo

c) založené na výslovnom súhlase dotknutej osoby.

[3] V prípadoch podľa odseku 2 písm. a) a c) je prevádzkovateľ povinný vykonať vhodné opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby, a to najmä práva na overenie rozhodnutia nie automatizovaným spôsobom zo strany prevádzkovateľa, práva vyjadriť svoje stanovisko a práva napadnúť rozhodnutie.

[4] Rozhodnutia podľa odseku 2 sa nesmú zakladať na osobitných kategóriách osobných údajov podľa § 16 ods. 1 okrem prípadov, ak sa uplatňuje § 16 ods. 2 písm. a) alebo písm. g) a súčasne sú zavedené vhodné opatrenia na zaručenie práv a oprávnených záujmov dotknutej osoby.“

Ostatné zvolili rôzne prístupy, čo viedlo k rozdielnom stupňom ochrany.[342]

[342] Viac pre porovnanie (Belgicko, Holandsko, Francúzsko, Nemecko, Maďarsko, Slovinsko, Rakúsko, Spojené kráľovstvo, Írsko) pozri Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations lGianclaudio Malgieri Computer Law & Security Review Volume 35, Issue 5, October 2019

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Potrebné je zdôrazniť, že ak členský štát povolí algoritmické riadenie, zamestnanec nebude mať k dispozícií katalóg práv (na ľudský zásah, vyjadriť svoje stanovisko a napadnúť rozhodnutie). Na zaručenie ochrany práv a slobôd a oprávnených záujmov dotknutej osoby musia národné legislatívy prijať vhodné opatrenia. Samotné GDPR však nevysvetľuje, o aké opatrenia by malo ísť.

Priestor na odlišné riešenia pri spracúvaní osobných údajov v súvislosti so zamestnaním poskytuje aj málo využívaný Článok 88, ktorý má pri rešpektovaní národných osobitostí zaistiť primeranú ochranu zamestnancov[343]:

1. Členské štáty môžu prostredníctvom právnych predpisov alebo kolektívnych dohôd stanoviť konkrétnejšie pravidlá na zabezpečenie ochrany práv a slobôd pri spracúvaní osobných údajov zamestnancov v súvislosti so zamestnaním, najmä na účely prijatia do zamestnania, plnenia pracovnej zmluvy vrátane plnenia povinností vyplývajúcich z právnych predpisov alebo kolektívnych zmlúv, ďalej na účely riadenia, plánovania a organizácie práce, rovnosti a rozmanitosti na pracovisku, ochrany zdravia a bezpečnosti pri práci, ochrany majetku zamestnávateľa alebo zákazníka, ako aj na účely uplatňovania a využívania práv a výhod súvisiacich so zamestnaním na individuálnom alebo kolektívnom základe, a na účely ukončenia pracovného pomeru.

2. Uvedené pravidlá zahŕňajú vhodné a osobitné opatrenia na zaistenie ľudskej dôstojnosti, oprávnených záujmov a základných práv dotknutej osoby s osobitným zameraním na transparentnosť spracúvania, prenos osobných údajov v rámci skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti a systémy monitorovania na pracovisku.

3. Každý členský štát oznámi Komisii do 25. mája 2018 ustanovenia svojich právnych predpisov, ktoré prijme podľa odseku 1, a bezodkladne oznámi aj všetky následné zmeny, ktoré sa ich týkajú.

[343] Bližšie pozri A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace Halefom H. Abraha, International Data Privacy Law, 2022, Vol. 12, No. 4 276-296.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Navyše, Článok 88 pripravuje právnu pôdu pre sociálnych partnerov, ktorí môžu zohrávať kľúčovú úlohu aj pri predchádzaní rizík algoritmického riadenia ľudských zdrojov. Kolektívne vyjednávanie sa javí ako najúčinnejší nástroj s prihliadnutím na to, ako rýchlo sa nové technológie vyvíjajú a zavádzajú na pracoviskách.[344]

9.5.2.6 Osobitné kategórie osobných údajov

Špeciálne osobné údaje sú vymedzené v Článku 9 ods. 1 GDPR: „Zakazuje sa spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby."

Ak spracúvanie zahŕňa tieto údaje, musia byť splnené požiadavky podľa odseku 4, a to buď výslovný súhlas s ich spracúvaním na účel automatizovaného rozhodovania, alebo spracúvanie je nevyhnutné z dôvodov významného verejného záujmu na základe práva Únie alebo práva členského štátu, ktoré sú primerané vzhľadom na sledovaný cieľ, rešpektujú podstatu práva na ochranu údajov a stanovujú vhodné a konkrétne opatrenia na zabezpečenie základných práv a záujmov dotknutej osoby.

V oboch prípadoch musí zamestnávateľ zaviesť primerané opatrenia na ochranu práv a slobôd a oprávnených záujmov zamestnancov.

9.5.2.7 Vhodné opatrenia

Ak sa zamestnávateľ spolieha na výnimku zmluvnej nevyhnutnosti alebo súhlasu, musí poskytnúť procedurálne garancie podľa odseku 3, ktorý treba čítať s odôvodnením 71 GDPR: *„V každom prípade by takéto spracúvanie malo podliehať vhodným zárukám, ktoré by mali zahŕňať* určité *informácie pre dotknutú osobu a právo na ľudský zásah, vyjadriť svoj názor,*

[344] DE STEFANO, V.: 'Master and Servers': Collective Labour Rights and Private Government in the Contemporary World of Work. International Journal of Comparative Labour Law and Industrial Relations, 36(4), 2020, 442

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

dostať vysvetlenie rozhodnutia, ktoré bolo prijaté po takomto posúdení, a napadnúť rozhodnutie.“

Zamestnanci majú právo:

- na ľudský zásah zo strany prevádzkovateľa,
- vyjadriť svoje stanovisko,
- dostať vysvetlenie rozhodnutia,
- napadnúť rozhodnutie

9.5.2.8 Kde sú zástupcovia zamestnancov?

Regulácia osobných údajov je vybudovaná na predpoklade, že zásah do súkromia sa dotýka jednotlivca. Umelá inteligencia je však čím ďalej sofistikovanejšia a čoraz viac zvýrazňuje nerovnovážne postavenie subjektov pracovnoprávneho vzťahu. Zamestnanci o jej zapojení do riadenia nemusia mať ani vedomosť. Ak sa aj o nej dozvedia, tak majú veľmi malú šancu pochopiť jej fungovanie, čo znamená, že ani nemôžu efektívne využívať svoje práva garantované GDPR. V neposlednom rade môže byť s uplatňovaním individuálnych práv spojený aj strach z odvetného postihu zo strany zamestnávateľa.

S cieľom posilniť transparentnosť, vysledovateľnosť a informovanosť je žiaduce pridať zástupcov zamestnancov do procesu implementácie a zmien, ktoré sa týkajú automatizovaných systémov. Zamestnávateľ by mal povinne poskytovať konzultácie o konkrétnych nastaveniach a parametroch algoritmov, ktoré môžu ovplyvňovať prístup k zamestnaniu, podmienky výkonu práce či udržanie si pracovnej pozície.

Ako vzor môže slúžiť *Real Decreto-ley 9/2021* z 11.05.2021. Ide o výsledok dohody medzi španielskou vládou, zástupcami zamestnancov a zamestnávateľov, ktorý zaviedol právo zástupcov zamestnancov na informácie a prerokovanie.[345]

9.5.2.9 Právo na ľudský zásah

[345] Viac pozri TODOLÍ-SIGNES, A.: Spanish riders law and the right to be informed about the algorithm.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Ani tento aspekt nie je úplne bez problémov. Upozorniť možno na obzvlášť hodný postreh Aloisiho: „[N]ie je jasné, kto by mal byť tento 'človek' a či bude môcť preskúmať proces, ktorý mohol byť založený na algoritmoch tretích strán, vopred naučených modeloch alebo súboroch údajov, vrátane osobných údajov iných osôb, alebo na nezrozumiteľných modeloch strojového učenia. Nie je ani jasné, či človek poverený preskúmaním rozhodnutia môže byť tá istá osoba, ktorá rozhodnutie prijala ako prvá, pričom stále môže podliehať tým istým vedomým alebo podvedomým predsudkom a predpojatostiam vo vzťahu k dotknutej osobe ako predtým.“[346]

9.5.2.10 Dôsledky nedodržania Článku 22

Určitou zábezpekou pred zneužitím môže byť aj potenciálna administratívna sankcia. Zamestnávatelia sa môžu zdráhať používať automatizované rozhodovacie systémy, ak im hrozí vysoká peňažná pokuta: „*Za porušenia práva dotknutých osôb podľa článkov 12 až 22 sa podľa odseku 2 uložia správne pokuty až do výšky 20 000 000 EUR, alebo v prípade podniku až do výšky 4 %* celkového *svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.*“[347]

[346] ALOISI, A.: Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context. Special Issue of Comparative Labor Law & Policy Journal, “Automation, Artificial Intelligence and Labour Protection”, edited by Valerio De Stefano, Vol. 41, No. 1, pp. 95-121 s. 114

[347] Článok 83 ods. 5 písm. b) GDPR.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

10 PRACOVNOPRÁVNE INŠTITÚTY SÚVISIACE S MONITOROVANÍM ZAMESTNANCOV

Monitorovanie zamestnancov prostredníctvom nových a sofistikovaných foriem kontroly na pracovisku môže mať priamy vplyv na samotných zamestnancov. S monitorovaním zamestnancov a rôznymi zásahmi do ochrany súkromia zamestnancov je priamo spojená problematika ďalších pracovnoprávnych inštitútov, ktoré súvisia s touto problematikou. Jedná sa o problematiku ľudskej dôstojnosti zamestnanca, problematiku vzniku stresu a technostresu ako následku neustáleho monitorovania zamestnancov alebo problematiku eliminácie digitálnych hrozieb na pracovisku ako napríklad šikany a kyberiškany prostredníctvom nových technológií a počítačových softvérov. V ďalej časti našej vedeckej analýzy sa preto zameriame na vybrané pracovnoprávne inštitúty, ktoré z hľadiska ich vecného obsahu priamo súvisia s problematikou monitorovania zamestnancov a nezákonných zásahov do ochrany súkromia zamestnancov.

10.1 DÔSTOJNOSŤ ZAMESTNANCA V PRACOVNOPRÁVNOM VZŤAHU

S monitorovaním zamestnancov priamo súvisí problematika dôstojnosti zamestnanca v pracovnoprávnych vzťahoch. Ľudská dôstojnosť zamestnanca môže byť narušená, pokiaľ sa monitorovanie zamestnanca alebo jeho výsledky uskutočňujú dehonestujúcim alebo ponižujúcim spôsobom, ktorý sa dotýka ľudskej dôstojnosti zamestnanca. Právo na ochranu ľudskej dôstojnosti nadobudlo osobitný význam najmä po prijatí Lisabonskej zmluvy. Ľudská dôstojnosť sa musí rešpektovať a chrániť. Výnimkou v tomto smere nie sú ani pracovnoprávne vzťahy, v rámci ktorých sa taktiež musí pri výkone práv a povinností rešpektovať právo na ľudskú dôstojnosť zamestnanca. Tento pojem má viacdimenzionálny rozmer a je súčasne centrálnym pojmom v katalógu ľudských práv upravených v Charte. Právo na ľudskú dôstojnosť patrí k základným ľudským právam a predstavuje základný stavebný kameň v práve EÚ. Ľudská dôstojnosť je nedotknuteľná a má svoje miesto aj v Európskom dohovore o ľudských právach a základných slobodách. Právo na rešpektovanie ľudskej dôstojnosti a samotným pojem ľudská dôstojnosť predstavuje požiadavku na právny výklad ľudských práv

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

optikou tohto pojmu, pričom takýmto právom nepochybne je aj ***právo na rešpektovanie súkromia zamestnanca.***

Právo zamestnanca na ochranu ľudskej dôstojnosti v pracovnoprávnych vzťahoch je možné v aplikačnej praxi používať aj pri ochrane práva na súkromný život zamestnanca v dôsledku neoprávnených zásahov do súkromia zamestnanca. Po nadobudnutí Lisabonskej zmluvy sa stala právne záväzná aj Charta, na ktorú sa Lisabonská zmluva priamo odvolávala s tým, že Charta je jej súčasťou. Na túto skutočnosť reagovala zahraničná literatúra, poukazujúc na doterajšiu judikatúru SD EÚ, že ak sa niektoré z práv zakotvených v Charte budú porušovať takýmto spôsobom, že ohrozia alebo porušia ľudskú dôstojnosť, musia byť žalovateľné na príslušnom vnútroštátnom súde.[348]

Z uvedeného vyplýva, že právo ochranu ľudskej dôstojnosti priamo súvisí s právom na ochranu súkromia zamestnanca. Právo na ochranu ľudskej dôstojnosti zamestnanca je priamym limitujúcim faktorom oprávnenosti zásahu do práva na súkromný a rodinný život zamestnanca. Pokiaľ zásah do súkromia zamestnanca narušil ľudskú dôstojnosť zamestnanca v pracovnoprávnych vzťahoch z hľadiska formy monitorovania, výsledkov monitorovania alebo skutkových a právnych následkov, takýto zásah má znaky nezákonného zásahu do ochrany súkromia zamestnanca, nakoľko takýmto monitorovaním bolo porušené právo na ochranu ľudskej dôstojnosti zamestnanca.[349]

10.2 DIGITÁLNE HROZBY NA PRACOVISKU A OCHRANA SÚKROMIA ZAMESTNANCA

S rozvojom nových digitálnych technológií sa čoraz viac možno stretnúť s problematikou digitálnych hrozieb na pracoviskách. Počet prípadoch digitálnych útokov voči zamestnancom sa s postupnou a masívnou digitalizáciou a internetizáciou zvyšuje. Digitálne útoky voči zamestnancom sa môžu uskutočňovať nie len na pracovisku zamestnávateľa, ale aj v domácom prostredí zamestnanca pri výkone domáckej práce alebo telepráce. Digitálne útoky sa môžu uskutočňovať na vertikálnej ako aj horizontálnej úrovni v rámci zamestnávateľa. Pri vertikálnych digitálnych útokoch a hrozbách sa najčastejšie vyskytujú

348 Rozsudok SD EÚ v právnej veci Stauder, C-29/69 zo dňa 12.11.1969, bod 419 odôvodnenia.

349 Nové technológie v pracovnoprávnych vzťahoch. Praha: Leges, 2017, str. 119, ISBN: 978-80-7502-253-0.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

útoky od zamestnávateľa, resp. vedúceho zamestnanca voči hierarchicky nižšie postaveným zamestnancom. Nie sú vylúčené prípady, kedy zamestnanec prostredníctvom digitálnych útokov atakuje nadriadeného zamestnanca, resp. priamo svojho zamestnávateľa.

Medzi dôvody takýchto digitálnych útokov možno zaradiť diskrimináciu na pracovisku z dôvodu rasy, sexuálnej orientácii, štátnej príslušnosti a národnosti alebo z dôvodu zdravotného stavu. Digitálne hrozby na pracovisku zamestnávateľa sa vyznačujú vysokým stupňom latentnosti pri ich odhaľovaní, pretože takého digitálne útoky sa uskutočňujú najčastejšie v anonymite alebo pod rôznymi pseudonymami za pomoci technických pomôcok na zmenu hlasu a intonácie tak, aby sa prípadná analýza hlasu digitálneho útočníka nedala pri znaleckom skúmaní analyzovať. Medzi súčasné digitálne hrozby súvisiace s ochranou súkromia zamestnanca patrí šikana a kyberiškana na pracovisku, digitálny *mobbing* a *bossing* na pracovisku, elektronický pokyn na diskrimináciu, sexuálne obťažovanie. Niektoré z uvedených digitálnych hrozieb môžu súčasne naplniť aj skutkové podstaty niektorých trestných činov taxatívne uvedených v osobitnej časti Trestného zákona.

10.2.1 Šikana a kyberšikana na pracovisku

Šikana v pracovnoprávnych vzťahoch je druh zneužitia práva, ktorý vyslovene zakazuje článok 2 Zákonníka práce, ktorý upravuje základné zásady. Podľa tohto článku Zákonníka práce musí byť výkon práv a povinností z pracovnoprávneho vzťahu v súlade s dobrými mravmi. V poslednom období prípadov šikany a kyberšikany na pracovisku zamestnanca stále viac pribúda. Takéto internetové útoky voči zamestnancom sú mnohokrát namierené proti ich ľudskej dôstojnosti, proti ich osobnosti alebo cielené proti ich rodinným príslušníkom.

Kyberšikana nemá svoju legislatívnu definíciu v slovenskom právnom poriadku. Vo svojej podstate sa jedná o spôsob šikany cez internet prostredníctvom digitálnych zariadení a aplikácií. Ide o novú formu šikany prostredníctvom nových informačno-komunikačných technológií, ako je napríklad mobil, plánovač úloh alebo iné digitálne aplikácie. Najčastejšie sa kyberšikana prejavuje tak, že zamestnancovi v postavení obete prichádzajú urážlivé a zosmiešňujúce e-maily pre nesplnenie pracovnej úlohy, zasielanie e-mailov a sms správ s vyhrážajúcim sa obsahom súvisiacim so skončením pracovného pomeru, vytváraním *tzv.*

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

black zoznamov kolujúcich na pracovisku zamestnávateľa s nedostatočnými výsledkami konkrétneho zamestnanca. Cieľom kyberšikany je vyvolanie strachu u zamestnanca a slúži k jeho úmyselnému ubližovaniu alebo ubližovaniu jeho rodinných príslušníkov.

Nie je vylúčené ani to, že takéto e-maily, sms správy alebo telefonáty sú vopred prednastavené v softvérových programoch zamestnávateľa, ktoré sú zasielané zamestnancom automatizovaným systémom majúcim za cieľ zlepšenie pracovných výsledkov zamestnanca pod hrozbou sankcie alebo interného pranierovania na pracovisku zamestnávateľa. Typickým príkladom môže byť spracovanie videozáznamu kamerovým systémom zamestnávateľa a jeho následné rozposielanie druhým zamestnancom zamestnávateľa s hrozbou, že aj oni môžu dostať výpoveď z pracovného pomeru, ak nebudú pracovať poriadne, rýchlo alebo sa budú zdržiavať dlhšie na fajčiarskej prestávke a pod.

Kyberšikana má oproti tradičnej šikane na pracovisku veľa spoločných znakov, avšak niektoré znaky sú typické len pre kyberšikanu. Proces šikanovania zamestnanca na pracovisku prostredníctvom informačno-komunikačných prostriedkov je realizovaný najmä v digitálnom prostredí, pričom zvyčajne súčasťou takejto šikany sú obrazové alebo obrazovo-zvukové záznamy získané v dôsledku nezákonného narušenia súkromia zamestnanca. Ďalším rozdielom medzi klasickou šikanou a kyberšikanou je, že pokým agresor pri klasickej šikane dominuje fyzickou silou, agresor pri počítačovej a kybernickej šikane dominuje znalosťami z oblasti informačno-komunikačných prostriedkov a zväčša vystupuje v anonymite. Zamestnanec v postavení kybernetickej šikany je vystavený zväčša väčšiemu okruhu ľudí ako pri klasickej šikane, pretože nezákonne získaný digitálny obsah takýchto útokov môže byť viditeľný širokému spektru adresátov, ktorými sú všetci zamestnanci zamestnávateľa. Typickým príkladom môže byť rozosielanie rôznych *newsletterov* všetkým zamestnancom zamestnávateľa, prostredníctvom ktorých dochádza ku kybernetickej šikane konkrétneho zamestnanca. Sú známe prípady, kedy zamestnávatelia prostredníctvom kybernetickej šikany šikanujú svojich zamestnancov tým, že im zasielajú podvodné e-maily a sms správy s nevhodným obsahom, že ak nezvýšia svoj pracovný výkon, tak oznámia zamestnávateľovi ich príbuzenský alebo rodinný vzťah s iným zamestnancom zamestnávateľa, nakoľko v rámci firemnej kultúry zamestnávateľa na tom istom pracovisku zamestnávateľa nemôžu pôsobiť

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

dvaja zamestnanci v príbuzenskom alebo v rodinnom zväzku, pričom k takémuto zisteniu dospeli nadriadení zamestnanci na základe nezákonného zásahu do súkromia zamestnancov prostredníctvom rôznych foriem ich monitorovania. Kybernetickú šikanu na pracovisku rozhodoval aj SD EÚ vo svojom rozhodnutí v právnej veci T-333/1999.[350]

10.2.2 Mobbing a bossing na pracovisku

Ďalšou formou digitálnej agresie na pracovisku je mobbing a bossing prostredníctvom informačno-komunikačných prostriedkov. Šikanovanie a mobbing so sebou priamo súvisia a predstavujú synonymné pojmy, pričom ich obsah nie je súladný s právnym poriadkom. Mobbing je viac zameraný na skupinové násilie a šikana je zameraná na jednotlivca na pracovisku. Mobbing je viac zameraný na psychické násilie na zamestnancovi, šikana je viac zameraná na fyzické násilie zamestnanca. Typickým príkladom kebyršikany môže byť pokyn zamestnávateľa na prácu súladnú s pracovnou zmluvou a jej náplňou, ktorá však nemá logické opodstatnenie v danej situácií a jej účelom je sankcionovanie zamestnanca tým, že bude vykonávať fyzicky alebo mentálne ťažkú prácu. Mobbing je širším pojmom ako šikana.

Medzi typické znaky mobbingu patrí napríklad systematickosť útokov, početnosť útokov, slabosť zamestnanca ako obete, početnosť rozličných správaní, vyčleňovanie zamestnanca z určitého kolektívu zamestnancov. Niektoré formy *mobbingu* môžu byť skutočne veľmi skryté a systematické, ktoré sa veľmi často v aplikačnej praxi dokazujú. Napríklad systematické vyčleňovanie zamestnanca z pracovného kolektívu nadriadeným zamestnancom môže byť skryté za časté nariaďovanie *home-officu* zamestnancovi, presun na iné zmeny, nariaďovanie pracovných ciest zamestnancovi, a to všetko za účelom čo najmenšieho trávenia na pracovisku zamestnávateľa, aby došlo k jeho exkomunikácií z kolektívu zamestnancov, v ktorom bol napríklad uznávanou a obľúbenou osobou. Obdobne to platí aj o bossingu. Bossing je jednou z foriem mobbingu, ktorý uskutočňuje nariadený zamestnanec alebo priamo zamestnávateľ voči podriadenému zamestnancovi. Jeho prejavy sú zastrašovanie a znižovanie ľudskej dôstojnosti zamestnanca na pracovisku.

[350] Rozsudok SD EÚ v právnej veci Pán X/ Európska centrálna banka, C – 333-1999 zo dňa 18.10.2001.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

10.2.3 Obťažovanie a sexuálne obťažovanie

Veľmi často na pracovisku zamestnávateľa dochádza k obťažovaniu zamestnanca zo strany iného zamestnanca alebo nadriadeného zamestnanca. Obťažovanie môže mať podobu fyzickú alebo psychickú v podobe neustáleho prenasledovania. Obťažovanie sa najčastejšie deje prostredníctvom internetu alebo digitálnych aplikácií. Zamestnancovi sú posielané správy s obsahom, ktoré rôznym spôsobom obťažujú zamestnanca s nezmyselnými otázkami alebo úlohami, ktoré rôznymi spôsobmi vyrušujú zamestnancov, v dôsledku čoho sa nedokážu plnohodnotne sústrediť na svoj výkon práce. Typickým príkladom je zasielanie e-mailov s odkazom na nákupy na internete alebo na stránky s nevhodným sexuálnym obsahom. Mnoho takýchto podvodných e-mailov je zasielaných zamestnancom s nečestným úmyslom, aby obeť klikla na takúto web stránku s nevhodným obsahom, pričom obťažovateľ vie, že obeť má monitorované stránky na počítači, a to s cieľom poukázať na to, že počas pracovnej doby pozerala web stránky s nevhodným alebo nesúvisiacim obsahom vzhľadom na jej pracovnú pozíciu. Obťažovanie môže alebo aj nemusí tvoriť obsah pojmu diskriminácia zamestnanca na pracovisku v zmysle antidiskriminačného zákona.

10.2.4 Digitálny pokyn na diskrimináciu

V súvislosti s nezákonnými zásahmi do súkromia zamestnanca sa veľmi často stáva, že zamestnávateľ alebo ním poverená osoba dá prostredníctvom informačno-komunikačných prostriedkov inému podriadenému vedúcemu zamestnancovi pokyn, aby niečo vykonala voči inému zamestnancovi. Vo svojej podstate sa jedná o nezákonný pokyn zachytený v digitálnom prostredí, ktorého obsah ani cieľ nie je v súlade s právnym poriadkom. Sme toho názoru, že už samotný pokyn na diskrimináciu je porušením antidiskriminačného zákona a preto je právne irelevantné, či osoba tento pokyn splnila alebo nesplnila. V aplikačnej praxi je problematika pokynov na diskrimináciu oveľa komplikovanejšia, a to z viacerých dôvodov. Spomedzi všetkých možno vyzdvihnúť, že samotná skutočnosť, že vedúci zamestnanec vydal pokyn na obťažovanie druhého zamestnanca automaticky neznamená, že vedúci zamestnanec, ktorý vydal takýto pokyn, obťažuje práve osobu, ktorej prikáže vykonať takýto pokyn. Pokyn na

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

obťažovanie druhého zamestnanca tak ako pokyn na diskrimináciu by mal byť považovaný za právny úkon, ktorý možno vyhodnotiť ako absolútne neplatný právny úkon a podľa Barancovej by mal byť napadnuteľný na súde.[351] Otázkou však zostáva, akým typom žaloby v zmysle Civilného sporového poriadku možno takýto pokyn napadnúť. Keďže v zmysle Civilného sporového poriadku už nemožno v zásade žalovať neplatnosť právneho úkonu, pokiaľ by takáto možnosť vyslovene nevyplývala z osobitného právneho predpisu, tak možno uvažovať napríklad o antidiskriminačnej žalobe v rámci antidiskriminačného sporu. Keďže však vydanie takéhoto pokynu jeho adresátovi neznamená, že osoba, ktorá pokyn na obťažovanie vydala tretej osoby, že automaticky ona diskriminuje adresáta pokynu. Adresát pokynu na obťažovanie (diskrimináciu) nie je aktívne legitimovaný na podanie antidiskriminačnej žaloby.

10.2.5 Monitorovacie programy ako prevencia pred digitálnym násilím

Na základe vyššie uvedených a popísaných digitálnych hrozieb sa zamestnávatelia snažia takýmto hrozbám zabrániť nainštalovaním rôznych počítačových a digitálnych softvérov, ktoré za pomoci ich algoritmických funkcií a umelej inteligencie dokážu vyššie popísané digitálne hrozby včas na pracovisku detekovať a odhaliť práve tým, že monitorujú obsah všetkých správ, hovorov a digitálneho správania sa zamestnanca na pracovisku. Takéto softvéry dokážu vyfiltrovať podozrivé správy a konania ich autorov a včas ich oznámiť priamo zamestnávateľovi alebo zodpovednému zamestnancovi. Sme toho názoru, že v tomto prípade dochádza ku kolízii práva zamestnanca na ochranu svojho súkromia ako aj práva na ochranu ľudskej dôstojnosti práve tým, že sú všetky jeho správy a digitálne kroky neustále monitorované, a právom zamestnávateľa na ochranu vlastníctva spolu s ďalšími zákonnými povinnosťami zamestnávateľa, ako napríklad povinnosťou zabezpečiť pre všetkých zamestnancov priaznivé, uspokojujúce a bezpečné pracovné podmienky.

Otázkou zostáva, ako by bolo takého neustále monitorovanie zamestnancov zamestnávateľa vyhodnotené zo strany všeobecných súdov ako súladné so zásadou legality, legitimity a proporcionality pri dodržaní zákonných povinností zamestnávateľa v zmysle § 13 ods. 4 Zákonníka práce, pretože v tomto prípade takéto monitorovanie zamestnancov a detekcia

[351] Nové technológie v pracovnoprávnych vzťahoch. Praha: Leges, 2017, str. 167, ISBN: 978-80-7502-253-0.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

potencionálnych páchateľov trestných činov spomedzi týchto zamestnancov prispieva k celospoločensky prospešnému cieľu, ktorým je prevencia pred páchaním trestnej činnosti.

10.3 Duševné zdravie zamestnanca a technostres

Starostlivosť o duševné zdravie zamestnanca sa pod vplyvom nových technológií stalo veľmi diskutovanou témou. S masívnou digitalizáciou a internetizáciou výrobných a pracovných postupov sa čoraz viac dostáva do popredia problematika duševného zdravia zamestnancov. Problematika duševného zdravia zamestnancov ovplyvnená neustálym narúšaním súkromia zamestnancov tým, ich zamestnávatelia neustále monitorujú, predstavuje len parciálnu časť širokej problematiky kvality duševného zdravia zamestnancov na pracovisku zamestnávateľa. Skutočnosť, že zamestnávateľ umožní svojim zamestnancov zamestnávateľa výkon práce z domáceho prostredia alebo ako formu telepráce, v sebe automaticky nesie možnosť kontroly zamestnávateľa kontrolovať výkon práce svojich zamestnancov. Kontrola zamestnancov sa môžu uskutočňovať prostredníctvom monitorovacích zariadení alebo prostredníctvom bežnej kontroly dostupnými technickými možnosťami bez potreby zavádzania osobitných monitorovacích zariadení. Typickým príkladom v tomto smere môže byť posielanie pravidelných správ a povinnosť zamestnanca v krátkej dobe na tieto správy odpovedať, byť dostupný stále online tak, aby na konkrétnej komunikačnej aplikácií stále svietil Váš status *„online“*, alebo prostredníctvom vizuálnej kontroly pripojenia Vášho počítača na firemnú sieť zamestnávateľa, kde zamestnávateľ v rámci systémových nastavení online siete vidí, že počítať zamestnanca je pripojený k jeho sieti. Neustále monitorovanie zamestnancov rôznymi spôsobmi nepochybne spôsobuje zvýšenú mieru **stresu zamestnanca**.

Pokiaľ k monitorovaniu zamestnancov dochádza prostredníctvom informačno-komunikačných prostriedkov, možno hovoriť o pojme *technostres*. Pojem *technostres* je dynamicky sa rozvíjajúcim pojmom, ktorý sa rovnako rýchlo mení a vyvíja, ako sa menia a vyvíjajú digitálne prostriedky slúžiace na výkon práce. Základným problémov nie je neznalosť informačno-komunikačných prostriedkov na výkon práce, ale ich predimenzovanosť a mimoriadna zaťaženosť na zamestnancov. Uvedené rovnako platí pre spôsoby

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

monitorovania zamestnancov zamestnávateľa. V oblasti psychiky sa strach zamestnanca z toho, že je neustále sledovaný, premieta napríklad v poruchách pamäti, koncentrácie, netrpezlivosťou, problémom s trávením odpočinku a relaxáciou, nakoľko zamestnanci sa častokrát domnievajú aj mimo práce, že sú monitorovaní. Medzi ďalšie zdravotné problémy môžeme zaradiť problémy s bolesťami hlavy. Z uvedeného dôvodu sa čoraz viac začínajú objavovať návrhy na uznanie technostresu ako choroby z povolania.[352] V tejto súvislosti možno uvažovať aj o širšom ponímaní práva na odpojenie sa[353], a to ***právo zamestnanca na odpojenia sa pred neustálym monitorovaním*** zo strany zamestnávateľa. Medzi právne prostriedky ochrany zamestnanca pred technostresom z dôvodu neustáleho monitorovania patrí sťažnosť zamestnávateľovi, zákazu obťažovania ako pojmovej súčasti širšieho zákazu diskriminácie alebo náhrady škody a náhrady nemajetkovej ujmy.[354]

[352] DOLOBÁČ, M.: Technostres a ochrana duševného zdravia zamestnanca. Str. 55. In: BARANCOVÁ, H., OLŠOVSKÁ, A. (eds.: Pracovné právo v digitálnej dobe. Praha: Leges, 2017, str. 58, ISBN: 978-80-7502-259-2.
[353] MORÁVEK, J.: Změny tradičných institutů a institucí v době 4.0 a jejich reflexe v rámci pracovnéprávn ílegislativy. Str. 43, In: BARANCOVÁ, H., OLŠOVSKÁ, A. (eds.): Priemysel 4.0 a pracovné podmienky. Praha: Leges, 2018, 128 s., ISBN: 978-80-7502-312-4.
[354] DOLOBÁČ M., SEILEROVÁ, M. (eds.): Starostlivosť o zdravie zamestnancov. Košice: Univerzita P. J. Šafárika v Košiciach, 2018, str. 85, ISBN: 978-80-8152-665-7.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

11 ZÁVERY - BUDÚCNOSŤ A PERSPEKTÍVA OCHRANY OSOBNÝCH ÚDAJOV A SÚKROMIA ZAMESTNANCA

11.1 ZOVŠEOBECŇUJÚCE ZÁVERY

Súčasná dynamicky sa vyvíjajúca digitalizácia a internetizácia výrobných procesov s flexibilnými formami zamestnávania so sebou prináša stále novšie a modernejšie spôsoby monitorovania zamestnancov, ktoré sú čoraz sofistikovanejšie. S novými spôsobmi monitorovania zamestnancov je spojené zvýšené riziko narušenia súkromia zamestnancov na pracovisku zamestnávateľa. Pri zavádzaní nových spôsobov monitorovania zamestnancov musia zamestnávatelia dodržať ustanovenie § 13 ods. 4 Zákonníka práce upravujúce podmienky pri zavádzaní monitorovacích mechanizmov u zamestnávateľa.

V rámci našej vedeckej analýzy sme poukázali na nové trendy v oblasti monitorovania zamestnancov. Medzi nové trendy v oblasti monitorovania zamestnancov patrí monitorovanie prostredníctvom softvérových a počítačových programov, monitorovanie prostredníctvom tzv. aktívnych odznakov alebo prostredníctvom umelej inteligencie, ktorá si na základe monitoringu zamestnanca dokáže sama pre zamestnávateľa vytvoriť personifikovaný profil zamestnanca o jeho zdravotnom stave, behaviórnom správaní a pod. Zamestnávateľ na základe takýchto personálnych profilov dokáže predikovať do budúcnosti určité situácie, ktoré sa môžu alebo nemusia naplniť. Typickým príkladom môže byť častá návšteva u konkrétneho lekára – špecialistu s indikáciou pre zamestnávateľa, že zamestnanec môže mať do budúcna určité zdravotné problémy súvisiace s oblasťou pôsobenia lekára – špecialistu. Nové trendy v oblasti monitorovania zamestnancov čoraz viac a sofistikovanejšie dokážu zbierať informácie o zamestnancoch zamestnávateľa, pričom výrazným posunom je, že za pomoci umelej inteligencie sú takého zozbierané informácie aj autonómne vyhodnocované pre zamestnávateľa.

Poukázali sme výnimky zo zásahov do ochrany súkromia zamestnanca, kedy takéto zásahy do súkromia zamestnancov nebudú predstavovať nezákonné konanie zo strany zamestnávateľa. Právo zamestnanca na ochranu súkromia je síce upravené v medzinárodných a európskych prameňoch práva, avšak uvedené právo nie je právom absolútnym a za vopred stanovených ústavných kritérií je možné aj toto právo zamestnanca obmedziť. Obmedziť právo

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

zamestnanca na ochranu súkromia v dôsledku nezákonného zásahu je možné len za splnenia podmienok legality, legitimity a proporcionality. Pokiaľ uvedený zásah do súkromia zamestnanca monitorovaním zamestnávateľa prejde testom legality, legitimity a proporcionality, uvedený zásah sa nebude považovať za nezákonný zásah do súkromia zamestnanca.

Na tomto mieste si dovoľujeme vyzdvihnúť nezastupiteľnú úlohu všeobecných súdov, ktoré budú rozhodovať o nezákonných zásahoch do práva na ochranu súkromia zamestnancov. Každý jeden prípad nezákonného zásahu do ochrany práva na súkromie bude potrebné posudzovať individuálne vzhľadom na oprávnené záujmy zamestnávateľa na monitorovaní zamestnanca, pričom ich budú všeobecné súdy posudzovať oproti oprávneným záujmom zamestnanca, medzi ktoré určite patrí právo na ochranu súkromia. V každom jednotlivom prípade je potrebné dôsledne skúmať, či zásah do ochrany práva na súkromie zamestnanca spĺňa podmienky legality, legitimity a proporcionality, pričom v rámci podmienky proporcionality je potrebné zamerať svoju činnosť na posúdenie, či uvedený a sledovaný cieľ zamestnávateľa nebolo v danom prípade možné dosiahnuť za menej invazívnych podmienok pri monitorovaní zamestnancov. Pri ochrane práva na súkromie zamestnancov zohráva veľkú úlohu rozhodovacia činnosť najvyšších súdnych autorít. Poukázali sme na rozhodovaciu činnosť Európskeho súdu pre ľudské práva, Ústavného súdu Slovenskej republiky ako aj zahraničných súdov, ktoré už prípady súvisiace s monitorovaním zamestnancov a nezákonnými zásahmi do práva na ochranu ich súkromia rozhodovali.

Zamestnávateľom pred zavádzaním kontrolných mechanizmov na pracovisku možno v tomto smere odporučiť, aby sa dôkladne pred inštaláciou týchto kontrolných mechanizmov oboznámili s ich technickými parametrami, nakoľko sa veľmi často stáva, že ani samotní zamestnávatelia nevedia, že ich softvérové programy alebo počítačové programy dokážu monitorovať ich zamestnancov do takej miery, že môže dochádzať k neoprávneným zásahom do ochrany práva na súkromie zamestnanca. Pokiaľ zo strany zamestnávateľa a zástupcov zamestnancov dôjde k prerokovaniu účelu, rozsahu a doby trvania monitorovania zamestnancov v zmysle § 13 ods. 4 Zákonníka práce, možno zúčastneným stranám odporučiť,

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

aby o dôsledkoch a rozsahu monitorovania zamestnancov informovali svojich zamestnancov v zrozumiteľnej forme a podobe.

Ďalej sme poukázali na osobitné kategórie zamestnancov, pri ktorých osobitná práva úprava rieši problematiku monitorovania zamestnancov. Poukázali sme na profesionálnych športovcov a športových odborníkov, pri ktorých zákon o športe upravuje osobitné podmienky pri ich monitorovaní a kontrole. Osobitná právna úprava monitorovania a kontroly profesionálnych športovcov je daná povahou činnosti práce, ktorú vykonávajú. Športová činnosť sa vyznačuje špecifickými vlastnosťami, ktoré odôvodňujú v oblasti športu benevolentnejší prístup v otázke ochrany súkromia profesionálnych športovcov a športových odborníkov. Rovnako tak sme poukázali na problematiku monitorovania zamestnancov v cestnej doprave prostredníctvom GPS systému s akcentom na problematické aspekty, medzi ktoré patrí monitorovanie polohy dopravného prostriedku v čase doby odpočinku alebo bezpečnostnej prestávky, ako aj problematika vymedzenia pracoviska pri mobilných zamestnancoch v cestnej doprave. Treťou analyzovanou osobitnou kategóriou zamestnancov boli sudcovia, ktorých výkon práce sa rovnako tak vyznačuje špecifickými vlastnosťami z oblasti etiky, morálky a verejného záujmu v nezávislé a nestranné rozhodovanie, ktoré sa niekedy môže dostať do kolízie s právom sudcu na ochranu jeho súkromia a s právom na ochranu jeho súkromného a rodinného života.

V našej analytickej štúdii sme sa zaoberali aj problematikou právnej ochrany zamestnanca pri porušovaní práva na ochranu jeho súkromia na pracovisku. Poukázali sme na vybrané právne inštitúty, ktorými sa zamestnanec môže domáhať nápravy nezákonného stavu. Pri sťažnosti zamestnanca sme poukázali na nie príliš vhodnú právnu úpravu v Zákonníku práce, kedy sťažnosť zamestnanca môžu v niektorých prípadoch slúžiť ako nástroj na šikovanie svojho zamestnanca pri domnelom alebo vymyslenom zásahu do práva na ochranu súkromia zamestnanca zo strany zamestnávateľa, nakoľko Zákonník práce neupravuje problematiku častých a opakovaných sťažností bez uvedenia nových relevantných dôvodov. Pokiaľ zamestnanec poukáže na nezákonné praktiky zamestnávateľa pri monitorovaní všetkých jeho zamestnancov vo veľkom rozsahu a obával by sa konzekvencií zo strany zamestnávateľa, môže

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

využiť inštitút chráneného oznamovateľa protispoločenskej činnosti, pokiaľ budú splnené ďalšie podmienky na jeho priznanie vyplývajúce z osobitného právneho predpisu.

Problematika nezákonných zásahov do práva na ochranu súkromia má interdisciplinárny charakter. Je tomu tak preto, pretože problematika nezákonných zásahov do ochrany súkromia zamestnanca je priamo prepojená s medicínskym hľadiskom, ktoré spočíva v následkoch takýchto zásahov do zdravotného stavu zamestnancov. V našej analytickej štúdii sme sa venovali problematike stresu a technostresu, ktoré môžu vyplývať z pocitu neustáleho monitorovania zamestnancov na pracovisku zamestnávateľa. Takéto zásahy do ochrany súkromia priamo súvisia s ľudskom dôstojnosťou fyzickej osoby v právnom postavení zamestnanca, ktorá je v dôsledku takýchto zásahov značne znížená.

Výkon práce prostredníctvom informačno-komunikačných prostriedkov v sebe zahŕňa aj možné digitálne hrozby na pracovisku zamestnávateľa. Medzi takého hrozby možno zaradiť napríklad kyberšikanu alebo digitálny pokyn na diskrimináciu alebo obťažovanie. Záverom sme poukázali na rôzne nové a softvérové a počítačové programy, ktoré dokážu eliminovať digitálne hrozby na pracovisku zamestnávateľa. Takého digitálne hrozby sú vyhodnocované prostredníctvom uvedených programov s umelou inteligenciou, ktorá dokáže detekovať správy, e-maily alebo telefonáty, ktoré napĺňajú definíciu kyberšikany alebo digitálneho pokynu na diskrimináciu iného zamestnanca. Za pomoci takýchto programov dokáže zamestnávateľ urýchlene prijať potrebné opatrenia na predchádzanie digitálnych hrozieb spojených s výkonom práce prostredníctvom informačno-komunikačných prostriedkov.

Na základe vyššie uvedeného vyplýva, že vlastnícke právo zamestnávateľa na kontrolu svojich výrobných a pracovných prostriedkov a ani právo na ochranu súkromia zamestnanca nie je právom absolútnym. V aplikačnej praxi je potrebné, aby sa uvedené práva aplikovali na pracovisku zamestnávateľa v rozumnej miere tak, aby uvedené práva boli v rovnováhe, navzájom sa rešpektovali a boli výsledkom vyváženosti práv a povinnosti medzi zamestnávateľom a zamestnancom v pracovnoprávnom vzťahu.

11.2 ZÁVERY K ROZHODOVACEJ PRAXI SÚDNYCH AUTORÍT

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Právo na ochranu osobných údajov je neoddeliteľnou súčasťou práv jednotlivcov a uplatňuje sa v situáciách, kde sa spracúvajú osobné údaje. Ochrana osobných údajov nie je obmedzená iba na oblasť súkromného života, ale týka sa všetkých typov osobných údajov a ich spracovania bez ohľadu na vzťah so súkromím. Spracovanie osobných údajov môže dokonca ovplyvniť aj právo na súkromie. Rozhodovacia činnosť Európskeho súdu pre ľudské práva (ESĽP) hrá kľúčovú úlohu pri interpretácii a uplatňovaní ochrany osobných údajov, a to najmä v kontexte zamestnania.

ESĽP rozvinul ochranu osobných údajov v súlade s technologickým pokrokom, ktorý umožnil získavať, spracúvať a využívať osobné údaje sofistikovanejším spôsobom. Vývoj judikatúry zohľadňuje nové metódy získavania údajov, ako aj vplyv technológií na ochranu osobných údajov.

ESĽP uznáva, že právo na ochranu osobných údajov je základným prvkom práva na rešpektovanie súkromného a rodinného života, obydlia a korešpondencie podľa článku 8 Dohovoru o ľudských právach. To znamená, že osobné údaje sú chránené nielen podľa špecifických ustanovení o ochrane údajov, ale aj v rámci širšieho kontextu práva na súkromie.

ESĽP definuje osobné údaje ako akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej osoby. Tieto údaje môžu byť priamo identifikujúce alebo nepriamo identifikujúce osobu. Príklady zahŕňajú mená, dynamické IP adresy, hlasové vzorky, bunkové vzorky DNA, údaje z bankových dokladov a ďalšie.

ESĽP posúdil rôzne typy operácií s osobnými údajmi v kontexte ochrany práva na súkromie. Patrí sem získavanie údajov o mieste pobytu, verejných informáciách o jednotlivcoch, uchovávanie hlasových vzoriek, monitorovanie GPS, filmovanie, záznamy z bezpečnostných kamier a ďalšie operácie.

ESĽP zdôraznil, že spracúvanie osobných údajov musí mať právny základ. Napríklad v pracovnom kontexte, spracovateľské operácie vyžadujú dodatočný právny základ, ako sú súhlas zamestnanca alebo právne povolenie.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ESĽP tak má kľúčovú úlohu pri interpretácii a uplatňovaní ochrany osobných údajov v rôznych kontextoch vrátane zamestnania. Rozvoj judikatúry zohľadňuje technologický pokrok a zabezpečuje ochranu osobných údajov v súlade s právom na súkromie a ľudskú dôstojnosť.

Rozhodovacia činnosť týkajúca sa zamestnaneckých vzťahov má dôležitý vplyv na ochranu osobných údajov a práva jednotlivcov. Zaznamenávanie a uchovávanie informácií o zamestnaní môže predstavovať zásah do práva na súkromie a rodinný život podľa článku 8 Európskeho dohovoru o ľudských právach. To platí pre akékoľvek informácie, ktoré sa týkajú identifikovateľnej osoby.

Osobné údaje v zamestnaní môžu zahŕňať posudky pracovného výkonu, ktoré obsahujú hodnotenie zamestnanca zo strany nadriadených. Tieto údaje môžu obsahovať aj osobné názory nadriadených, ktoré sa týkajú pracovného výkonu zamestnanca. Je dôležité poznamenať, že aj takéto hodnotenia sú považované za osobné údaje, ktoré podliehajú ochrane.

Spracúvanie osobných údajov v pracovnom kontexte vyžaduje primeraný právny základ, ako je súhlas zamestnanca alebo iné právne povolenie. Tým sa zabezpečuje, že zaznamenávanie a uchovávanie týchto údajov je v súlade so zákonom.

Súčasné automatické spracovanie údajov, ktoré sa týka zamestnancov, má potenciálne vážne dôsledky. Tieto údaje môžu byť ľahko prístupné a prenosné, čo môže mať negatívny vplyv na povesť jednotlivcov alebo ovplyvniť ich každodenný život.

Štát nesmie delegovať svoje povinnosti na súkromné subjekty ani jednotlivcov. Ak súkromný subjekt vykonáva činnosti, ktoré sú podobné verejným úlohám, môže byť považovaný za orgán verejnej moci a jeho činy sú pričítateľné štátu.

Preskúmanie, či zásah do práva na súkromie bol oprávnený, sa zakladá na troch kritériách: zákonnosť, legitímny cieľ a nevyhnutnosť v demokratickej spoločnosti. Tieto kritériá sa uplatňujú vo všetkých prípadoch, kde dochádza k zásahu do práva na súkromie.

Vo vzťahu k zhromažďovaniu údajov ESĽP posudzoval zhromažďovanie osobných údajov zamestnancov z verejného a súkromného sektora. Zber údajov mohol byť buď utajený, alebo

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

čiastočne utajený. Osobné údaje sa zbierali z rôznych zdrojov, ako sú telefonické hovory, používanie telefónu, e-mailu, internetu na pracovisku a videonahrávky správania na pracovisku.

Vo vzťahu k právu na súkromie ESĽP rozhodol, že osobné údaje zahŕňajú aj súkromný život zamestnancov. Zamestnanci by mali byť informovaní o možnostiach monitorovania a zásahov do ich súkromia. Transparentnosť a informácie o monitorovaní majú kľúčový význam pre ochranu práva na súkromie.

K legitímnym dôvodom patrí existencia dôvodného podozrenia a rozsah strát môžu byť dôvodom pre zamestnávateľa na zber údajov na pracovisku.

Zamestnávateľ by mal uplatňovať opatrenia zberu údajov s ohľadom na ich primeranosť a ochranu súkromia zamestnancov.

Kritériá pre dohľad nad zamestnancami vyplývajú z kritérií pre opatrenia dohľadu, vrátane informovania zamestnancov, rozsahu monitorovania, dôvodov na monitorovanie a existencie alternatívnych, menej rušivých metód. Transparentnosť a právo na informácie sú kľúčové pri dohľade nad komunikáciou zamestnancov na pracovisku. Zamestnanci by mali byť informovaní o možnostiach dohľadu a mali by mať prístup k opravným prostriedkom pri porušení ich práv. Očakávania ohľadom ochrany súkromia závisia na konkrétnych pracovných prostrediach, pričom súkromie je vysoko chránené na súkromných miestach a nižšie na miestach prístupných verejnosti. Zamestnávateľ by mal uplatňovať opatrenia dohľadu zohľadňujúce potreby a práva zamestnancov a zabezpečiť primerané záruky.

Uchovávanie informácií o súkromnom živote jednotlivca orgánmi verejnej moci je zásahom do práva na rešpektovanie súkromného života dotknutej osoby podľa článku 8 Dohovoru o ochrane ľudských práv a slobôd. Tento zásah vyžaduje dôkladné preskúmanie akéhokoľvek štátneho opatrenia, ktoré umožňuje uchovávanie a používanie osobných údajov bez súhlasu dotknutej osoby. Príkladom je prípad *M.M. proti Spojenému kráľovstvu*, kde sa riešili dôsledky zmien politiky týkajúcej sa doby uchovávania osobných údajov v registri trestov v súvislosti s vyhliadkami na zamestnanie. V tomto prípade sa zdôraznila potreba jasných a podrobných zákonných predpisov, ktoré by upravovali trvanie uchovávania týchto údajov.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ESĽP sa v niekoľkých prípadoch zaoberal opatreniami, ktoré zahŕňajú sprístupnenie osobných údajov jednotlivca iným subjektom. V prípade zverejnenia údajov na ochranu verejného zdravia sa zohľadnilo právo osoby na rešpektovanie lekárskeho tajomstva v súvislosti s potrebou ochrániť základné záujmy verejnosti a zamestnancov nemocnice.

V prípade zverejnenia údajov na ochranu národnej bezpečnosti ESĽP zdôraznilo, že aj keď boli osobné údaje sťažovateľa zverejnené s jeho súhlasom, stále sa musí preskúmať, či bol daný jednotlivec vystavený náležitým zárukám a či sa zachovala rovnováha medzi jeho právami a verejným záujmom. V prípade *Sõro proti Estónsku* sa zohľadnila zmena okolností a postoj kolegov sťažovateľa, ktorý ukázal závažnosť zásahu do jeho práva na súkromie.

Skutočnosť, že osobné údaje sú zverejnené na základe súhlasu jednotlivca, nezbavuje tieto údaje ochrany. Je dôležité, aby jednotlivci mali skutočnú možnosť výberu a aby existovali dostatočné záruky týkajúce sa trvania a rozsahu zverejnených údajov.

Ochrana osobných údajov v kontexte práva na spravodlivý proces. Právo na spravodlivý proces je základným právom, ktoré je chránené podľa článku 6 ods. 1 Európskeho dohovoru o ľudských právach. Toto právo zabezpečuje, že každý jednotlivec má nárok na spravodlivé, verejné a primerané súdne konanie pred nezávislým a nestranným súdom.

Všeobecné záruky práva na spravodlivý proces sú zakotvené v článku 6 ods. 1 Dohovoru. Európsky súd pre ľudské práva vo viacerých prípadoch posudzoval potrebu ochrany osobných údajov strán alebo tretích osôb v kontexte rôznych všeobecných záruk určených na zabezpečenie spravodlivosti súdneho konania. Tieto záruky zahŕňajú rovnosť zbraní a právo na kontradiktórne konanie, právo na verejné prejednanie veci a verejné vyhlásenie rozsudku, dokazovanie, primeranú dĺžku konania a požiadavku na odôvodnenie súdnych rozhodnutí.

V prípade *Eternit proti Francúzsku* sa ESĽP zaoberal situáciou, kde zamestnávateľ žiadal kópiu vyjadrenia lekárskeho poradcu poisťovne v súvislosti s chorobou jedného zo svojich zamestnancov. Súd dospel k záveru, že neposkytnutie tejto informácie zamestnávateľovi bolo odôvodnené ochranou dôvernosti zdravotných údajov a neporušilo právo na spravodlivý proces podľa článku 6 ods. 1.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Prípad *Surikov proti Ukrajine* poukázal na potrebu vnútroštátnych súdov zdôvodňovať svoje rozhodnutia. ESĽP zdôraznil, že zásada spravodlivosti si vyžaduje, aby súdy zohľadnili konkrétne a relevantné body sťažovateľa pri zdôvodňovaní svojich rozsudkov.

ESĽP sa v niekoľkých prípadoch zaoberal použitím osobných údajov, ktoré boli zhromaždené nezákonne alebo v rozpore s právom alebo článkom 8 Dohovoru, ako dôkazu vo súdnych konaniach. Toto zahrňuje prípady, kde informácie boli získané od poisťovní, zamestnávateľov alebo tajnou políciou.

Dĺžka súdnych konaní je kľúčovým aspektom práva na spravodlivý proces. ESĽP rozhodol, že extrémne dlhé konanie môže byť v rozpore s článkom 6 ods. 1.

Podľa článku 13 Dohovoru má každý právo na účinný prostriedok nápravy v prípade porušenia svojich práv ustanovených Dohovorom. Toto právo zabezpečuje, že jednotlivci majú možnosť žiadať nápravu a ochranu pred neoprávneným zásahom do svojich práv.

Celkovo sa ochrana osobných údajov v kontexte práva na spravodlivý proces stáva dôležitým aspektom v rámci zabezpečenia ľudských práv a súdnej spravodlivosti.

Právna regulácia týkajúca sa prístupu k dokumentom EÚ a ochrany osobných údajov predstavuje dôležitý aspekt v rozhodovacej činnosti aj Súdneho dvora EÚ. Záujem o transparentnosť a prístup k dokumentom sa musí vyvážiť s právom na ochranu osobných údajov.

Získavanie údajov o pracovnom príjme jednotlivca: Súdny dvor EÚ sa už viackrát venoval konfliktu medzi právom na prístup k dokumentom a právom na ochranu osobných údajov. V prípade *Rechnungshof/Österreichischer Rundfunk a i.* sa riešila zlučiteľnosť rakúskych právnych predpisov s právom EÚ o ochrane údajov. Súdny dvor zdôraznil význam ochrany základných práv a potrebu vyvážiť legitímne ciele súvisiace s transparentnosťou so záujmami na ochrane osobných údajov. Tento prípad poukazuje na dôležitosť náležitého zváženia pri prístupe k osobným údajom v dokumentoch verejných subjektov.

Záznamy o pracovnom čase a ochrana údajov: V súvislosti s právom zamestnancov na ochranu osobných údajov sa Súdny dvor zaoberal aj záznamami o pracovnom čase. Nariadenie o

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ochrane údajov stanovuje, že zamestnanci by mali mať jasný prehľad o spracúvaní ich údajov a ich právach. Súdny dvor podčiarkol, že porušenie ochrany osobných údajov môže viesť k vážnemu riziku pre práva jednotlivcov. Vnútroštátne orgány majú možnosť stanoviť dodatočné pravidlá na ochranu týchto práv v rámci zamestnania. Prípad *Worten* ukazuje, že spracovanie údajov o pracovnom čase musí rešpektovať zásady ochrany údajov a informovať zamestnancov o ich právach.

Súdny dvor EÚ zohľadňuje komplexné právne záležitosti týkajúce sa prístupu k dokumentom a ochrany osobných údajov, pričom jeho rozhodnutia majú dôležitý vplyv na zabezpečenie vyváženého a zákonného prístupu k informáciám v rámci EÚ.

Nezávislé súdne posúdenie ochrany osobných údajov vo vzťahoch medzi zamestnanom a zamestnávateľom preto hrá kľúčový význam z viacerých dôvodov:

Zabezpečuje práva zamestnanca: Nezávislý súdny proces zabezpečuje, že zamestnanec má možnosť brániť svoje práva v prípade porušenia ochrany osobných údajov. Ak sa vyskytne spor medzi zamestnancom a zamestnávateľom ohľadom ochrany údajov, súd môže rozhodnúť v súlade s platnými zákonnými predpismi a ochrániť práva jednotlivca.

Zamedzuje zneužitiu moci zamestnávateľa: Nezávislý súdny proces zabraňuje zneužitiu moci zo strany zamestnávateľa. Zamestnávatelia majú prístup k citlivým osobným údajom svojich zamestnancov, a tak je dôležité, aby existoval mechanizmus, ktorý zabezpečuje, že tieto údaje nebudú zneužité na nevhodné účely.

Posilňuje transparentnosť: Súdne posúdenie ochrany osobných údajov prispieva k transparentnosti v procese a umožňuje verejnosti lepšie porozumieť tomu, ako sa s osobnými údajmi v zamestnaní nakladá. To pomáha budovať dôveru v systém ochrany údajov.

Prináša právnu istotu: Nezávislé súdne rozhodnutie poskytuje právnu istotu a jasné usmernenia pre zamestnávateľov a zamestnancov týkajúce sa ochrany osobných údajov v pracovnom prostredí. To umožňuje organizáciám a jednotlivcom plniť svoje zákonné povinnosti a práva v tejto oblasti.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

Dohľad nad súladom so zákonom: Súdne posúdenie umožňuje zabezpečiť, že organizácie dodržiavajú platné zákony a predpisy týkajúce sa ochrany osobných údajov v zamestnaní.

Riešenie komplexných sporov: Niektoré spory týkajúce sa ochrany osobných údajov môžu byť komplexné a vyžadovať podrobné vyšetrovanie a riešenie. Nezávislý súd disponuje potrebnými zdrojmi a odbornosťou na vykonávanie takýchto vyšetrovaní a rozhodovanie o sporných otázkach.

Celkovo nezávislé súdne posúdenie ochrany osobných údajov v zamestnaní je kritické pre zachovanie rovnováhy medzi právami a záujmami zamestnancov a zamestnávateľov v tejto citlivej oblasti a zabezpečuje, že ochrana osobných údajov je efektívna a spravodlivá.

11.3 ZÁVERY K OCHRANE SÚKROMIA V INTENCIÁCH GDPR A ZÁKONA O OCHRANE OSOBNÝCH ÚDAJOV

Na spracúvanie osobných údajov v rámci pracovnoprávnych vzťahov sa aplikuje všeobecná právna úprava ochrany osobných údajov, ktorá je na úrovní EÚ prezentovaná v podobe GDPR. Zamestnávatelia sú vo väčšine prípadov v postavení prevádzkovateľa a nesú zodpovednosť za súlad s pravidlami na ochranu osobných údajov.

Z hľadiska kľúčových povinností sme osobitne zvýraznili správne vymedzenie účelu a právneho základu spolu so súladom so základnými zásadami spracúvania osobných údajov. Medzi typické účely spracúvania osobných údajov z pohľadu zamestnávateľov sme uviedli účely personalistiky a mzdy, bezpečnosť a ochrana majetku, monitorovacie mechanizmy zamestnávateľa, daňové a účtovné účely, zverejňovanie informácií o zamestnancoch a zákonné povinnosti zamestnávateľa.

Pri analýze právnych základov sme pre tieto účely vymedzili vhodné právne základy. Navyše, osobitne sme uviedli, že súhlas v pracovnoprávnych vzťahoch ako právny základ v drvivej väčšine prípadov nie je vhodným právnym základom, nakoľko narušuje slobodu jeho udelenia pri zamestnancovi ako zraniteľnej alebo slabšej strane.

Zároveň sme upozornili na porušenia základných zásad spracúvania osobných údajov v prípadoch, ktoré sa týkali monitorovania na pracovisku, nedostatočnej bezpečnosti alebo

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

porušenia zákonnosti pri spracúvaní osobných údajov. Zvýraznili sme aj relevantnosť inštitútov ako posúdenie vplyvu na ochranu údajov a zodpovedná osoba pre zamestnávateľov.

Slovenský zákon o ochrane osobných údajov nie je dobre koncipovaná právna úprava. V prvom rade nevyužíva priestor na vlastnú úpravu v podobe otvorených klauzúl, ktoré mu GDPR umožňuje. V druhom rade, ak nejaké otvorené klauzuly využíva, robí to veľmi všeobecným a neefektívnym spôsobom. Z tohto dôvodu považujeme za vhodné koncepčne zmeniť zákon o ochrane osobných údajov takým spôsobom, aby vyššie uvedené nedostatky odstraňoval.

Sme presvedčení, že po vzore nemeckej právnej úpravy by sa zákonodarca mal inšpirovať pri využití otvorenej klauzuly v pracovnoprávnych vzťahoch. Nemal by sa zamerať iba na sprístupňovanie určitých údajov, ako to robí súčasný zákon o ochrane osobných údajov, ale zohľadniť aj možnosti spracúvania údajov týkajúcich sa zdravia a ich okolností či možného monitorovania priestorov zamestnávateľa za účelom ochrany majetku a v tejto súvislosti aj vyjasnení limitov § 13 ods. 4 zákona č. 311/2001 Z. z. Zákonníka práce. Niektoré špecifiká spracúvania osobných údajov v pracovnoprávnych vzťahoch by mali byť reflektované prostredníctvom osobitných pravidiel. GDPR na to ponúka priestor, ktorý slovenský zákonodarca zatiaľ nevyužil.

11.4 K OTÁZKE ROZŠÍRENIA OCHRANY OSOBNÝCH ÚDAJOV NA PRÁVNICKÉ OSOBY

Napriek tomu, že ochrana osobných údajov sa obmedzuje v podstate iba na fyzické osoby, stojí za uváženie, či by sa nemala poskytovať aj právnickým osobám. Právo na ochranu údajov by sa tak mohlo vzťahovať aj na spracúvanie dôverných informácií právnickej osoby. V kontexte pracovnoprávnych vzťahov by to mohlo byť zaujímavé nielen pre zamestnávateľov, ale najmä pre odborové organizácie.

Tejto možnosti je otvorený aj Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov z 28. januára 1981, ktorý nadobudol platnosť v roku 1985 a bol aktualizovaný v roku 2018. V dôvodovej správe sa uvádza, že „*strany* [pozn.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

členské štáty] *môžu rozšíriť ochranu vo svojom vnútroštátnom práve na údaje týkajúce sa právnických osôb, aby ochránili ich oprávnené záujmy*“[355].

Aj usmernenia Organizácie pre hospodársku spoluprácu a rozvoj z roku 2013 v zásade pracujú s touto možnosťou, ale pre chýbajúcu zhodu na nadnárodnej úrovni, ponechávajú túto otázku otvorenú. OECD uvádza, že „*skúsenosti z viacerých krajín tiež ukazujú, že je ťažké jasne definovať deliacu čiaru medzi osobnými a neosobnými údajmi. Napríklad údaje týkajúce sa malej firmy sa môžu týkať aj jej vlastníka alebo vlastníkov a môžu poskytovať osobné informácie viac či menej citlivého charakteru. V takýchto prípadoch môže byť vhodné rozšíriť ochranu poskytovanú pravidlami, ktoré sa týkajú predovšetkým osobných údajov, aj na právnické osoby. (...) Niektorí členovia expertnej skupiny navrhli, aby sa zabezpečila možnosť rozšírenia usmernení na právnické osoby (korporácie, združenia). Na tomto návrhu nebol zabezpečený dostatočný konsenzus. Rozsah usmernení je preto obmedzený na údaje týkajúce sa jednotlivcov a je ponechané na členské štáty, aby nakreslili deliace čiary a rozhodovali o politikách s ohľadom na korporácie, skupiny a podobné orgány*“.[356]

[355] Explanatory Report, bod 30: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[356] The OECD Privacy Framework, 2013, bod 49: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] ABRAHA, H. Regulating algorithmic employment decisions through data protection law. s. 9

[2] ADAMIČKA, M., DIVÉKYOVÁ, K., POBIJAK, T.: Konanie podnikateľa. Praha: Wolters Kluwer ČR, 2020, 120 s.

[3] ALOISI, A. – POTOCKA-SIONEK, N.: De-gigging the labour market? An analysis of the 'algorithmic management' provisions in the proposed Platform Work Directive, Italian Labour Law e-Journal Issue 1, Vol. 15 (2022) s. 39

[4] ALOISI, A.: Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context. Special Issue of Comparative Labor Law & Policy Journal, "Automation, Artificial Intelligence and Labour Protection", edited by Valerio De Stefano, Vol. 41, No. 1, pp. 95-121 s. 114

[5] BAJÁNKOVÁ, J., VOJČÍK, P. Neplatnosť právnych úkonov a rozhodovacia prax súdov. In: Ingerencia súdov do súkromnoprávnych zmlúv: Zásahy súdov do obsahu súkromnoprávnych zmlúv. Pezinok: Justičná akadémia Slovenskej republiky, 2014, s. 20.

[6] BARANCOVÁ, H. a kol.: Ochrana zamestnanca, súčasnosť a budúcnosť pracovného práva. 1. vyd., Bratislava: Sprint dva, 2012, 54 s., ISBN: 978-80-89393-66-4.

[7] BARANCOVÁ, H. a kol.: Pracovný pomer a poistný systém. Bratislava : Typi Universitatis Tyrnaviensis, vydavateľstvo Trnavskej univerzity, Veda - Vydavateľstvo Slovenskej akadémie vied, 2008, s. 413.

[8] BARANCOVÁ, H. a kol.: Základné práva a slobody v pracovnom práce. Plzeň: Aleš Čeněk, 2012. 118 s., ISBN: 97-80-7380-422-0.

[9] BARANCOVÁ, H. Zákonník práce. Komentár 4. vydanie. Bratislava : C.H. Beck, 2015.

[10] BARANCOVÁ, H., OLŠOVSKÁ, A (eds.): Pracovné právo v digitálnej dobe. Praha: Leges, 2017, s. 70

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[11] BARANCOVÁ, H., SCHRONK, R. Pracovné právo, Bratislava SPRINT 2007, ISBN: 978-80-89085-95- 8.

[12] BARANCOVÁ, H., SCHRONK, R.: Pracovné právo. Druhé prepracované a doplnené vydanie. Bratislava: Sprint 2, 2013, str. 259, ISBN: 978-80-89393-97-8.

[13] BARANCOVÁ, H.: Monitorovanie zamestnancov a ochrana súkromného života v judikatúre európskych súdov. In: Justičná revue, 63, 2011, č. 3, s. 340.

[14] BARANCOVÁ, H.: Nové technológie v pracovnoprávnych vzťahoch. Praha: Leges, 2017, ISBN: 978-80-7502-253-0.

[15] BARANCOVÁ, H.: Práva zamestnancov Európskej únie. Praha: Leges, 2016, ISBN: 978-80-7502-117-5.

[16] BARINKOVÁ, M. - ŽUĽOVÁ, J: Elektronizácia pracoviska s akcentom na ochranu práva zamestnanca a zamestnávateľa. In: Právo, obchod, ekonomika VI. : zborník príspevkov z vedeckej konferencie. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2016.

[17] BERTHOTY, J. a kol. : Všeobecné nariadenie o ochrane osobných údajov. C.H. Beck. Praha, 2018.

[18] CALLAND, R., DEHN, G.: Whistleblowing Around the World: Law Culture and Practise, IDASA Publishers, p. 9, ISBN: 978-19-19798-56-1.

[19] CÍSAŘOVÁ, E.: Whistleblowing a ochrana oznamovatelů v České republice, Praha: Transparency International, str. 7, ISBN: 978-80-87123-11-9.

[20] ČAPEK, J.: Z rozhodnutí Evropského soudu a Evropské komisie pro lidská práva (Ochrana soukromného a rodinného života, obydlí a korespondence)– část VII; Právní praxe, r. XLIII., 1995, č. 7, s. 430-432.

[21] DE STEFANO, V.: 'Master and Servers': Collective Labour Rights and Private Government in the Contemporary World of Work. International Journal of Comparative Labour Law and Industrial Relations, 36(4), 2020, 442

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[22] DOLOBÁČ M., SEILEROVÁ, M. (eds.): Starostlivosť o zdravie zamestnancov. Košice: Univerzita P. J. Šafárika v Košiciach, 2018, str. 85, ISBN: 978-80-8152-665-7.

[23] DOLOBÁČ, M.: Technostres a ochrana duševného zdravia zamestnanca. Str. 55. In: BARANCOVÁ, H., OLŠOVSKÁ, A. (eds.: Pracovné právo v digitálnej dobe. Praha: Leges, 2017, str. 58, ISBN: 978-80-7502-259-2.

[24] DRGONEC, J.: Právo na súkromie podľa Ústavy Slovenskej republiky. Časopis pro právní vědu a praxi, 2000, ročník VIII., č. 2, s. 203 – 212. FILIP, J.: K otázce ústavní ochrany společnosti a státu de lege lata a de lege ferenda. Časopis pro právní vědu a praxi, II., 1996, č.4, s. 631 – 634.

[25] DRGONEC, J.: Ústava Slovenskej republiky. Komentár. Teória a prax. 1. vyd. Bratislava: C.H. Beck, 2015, str. 538, ISBN: 978-80-89603-39-8.

[26] FEILER, L. – FORGÓ, N. – WEIGL, M.: The EU General Data Protection Regulation (GDPR): A Commentary. Globe Law and Business, 2018, s. 30.

[27] FEILER, L.: Öffnungsklauseln in der Datenschutz-Grundverordnung - Regelungsspielraum des österreichischen Gesetzgebers. Dostupné na: https://lesen.lexisnexis.at/_/oeffnungsklauseln-in-der-datenschutz-grundverordnung-regelungssp/artikel/jusit/2016/5/jusIT_2016_05_093.html.

[28] FUREK, A., JIROVEC, T. § 3. In FUREK, A., ROTHANZL, L., JIROVEC, T. Zákon o svobodném přístupu k informacím. 1. vydání. Praha : C. H. Beck, 2016, s. 175.

[29] GALVAS, M. a kol.: Pracovní právo. Vyd. 1. Brno : Masarykova univerzita, 2012, s. 601.

[30] HAMUĽÁK, J.: Zmeny v právnej úprave Zákonníka práce – analýza a úvaha o platných a pripravovaných zmenách. Zborník príspevkov z medzinárodnej konferencie doktorandov a mladých vedeckých pracovníkov organizovanej Univerzitou Komenského v Bratislave, Právnickou fakultou. „Míľniky práva v stredoeurópskom priestore“ Bratislava: PrafUK, 2011, 724 s.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[31] HIJMANS, H. Article 51. In KUNER, CH. a kol. The EU General Data Protection Regulation (GDPR). A commentary. Oxford University Press, 2020.

[32] HOLLÄNDER, P.: Základy všeobecné státovědy, 2. rozšírené vydanie. Plzeň: Aleš Čeněk, 2009, 364 s.

[33] HORVAT, M. In Cepek, B. a kol. Správne právo hmotné. Všeobecná časť. Bratislava : Wolters Kluwer, 2018, s. 74.

[34] HROMADA, M.: Ochrana osobnosti zaměstnance při elektronické komunikaci. str. 161. In: BARANCOVÁ, H., OLŠOVSKÁ, A. (eds.): Pracovné právo v digitálnej dobe. Praha: Leges, 2017, 304 s., ISBN: 978-80-7502-259-2.

[35] HUDECOVÁ, I. – CYPRICHOVÁ, A. – MAKATURA, I. a kol.: Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár. Eurokódex, 2018.

[36] IKRÉNYI, P. a kol. Zákon o slobodnom prístupe k informáciám. Komentár. Bratislava : Wolters Kluwer, 2015, s. 23.

[37] IVANČÍK, J. Rozšírenie okruhu povinných osôb v oblasti práva na informácie po legislatívnych zmenách v roku 2022. In Acta Facultatis Iuridicae Universitatis Comenianae, Vol. 42, č. 1 (2023), s. 59-60.

[38] KAMARINOU, D., MILLARD, CH., SINGH, J.: Machine Learning with Personal Data (November 7, 2016). Queen Mary School of Law Legal Studies Research Paper No. 247/2016, s. 15

[39] KMEC, J., KOSAŘ, D., KRATOCHVÍL, J., BOBEK, M.: Evropská úmluva o lidských právech. Komentář. Praha: C .H. Beck, 2012, str. 99.

[40] KOŠIČIAROVÁ, S. In DOBROVODSKÝ, R., KOŠIČIAROVÁ, S. Právo na informácie. Krakov : Spolok Slovákov v Poľsku, 2015, s. 16.

[41] KOŠIČIAROVÁ, S. Správne právo hmotné. Všeobecná časť. Plzeň : Aleš Čeněk, 2022, s. 90

[42] KRIŽAN, V.: Ochrana súkromia zamestnanca v ére internetu. In: BARANCOVÁ, H., OLŠOVSKÁ, A. (eds.): Súčasný stav a nové úlohy pracovného práva. Zborník vedeckých

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

príspevokov z medzinárodnej konferencii Trnavské právnické dni. Trnava. 2016, Praha: Leges, 2016, 260 s. a nasl., ISBN: 978-80-7502-176-2.

[43] KRIŽAN, V.: Pracovná cesta vs. pracovný čas vyslaného zamestnanca, str. 91. In: VOJTKO, J.: Ochrana zamestnancov pri ich vyslaní do krajín Európskeho hospodárskeho priestoru. Zborník príspevkov z on-line konferencie. Trnava: Trnavská univerzita v Trnave, Právnická fakulta, 2015, 109 s., ISBN: 978-80-8082-936-0.

[44] KURIL, M. Procesná autonómnosť pracovného práva - quo vadis? In: KURIL. M. Zákon č. 311/2001 Z.z. Zákonník práce desať rokov aplikačnej praxe (2001-2011) : zborník vedeckých článkov – 1. vyd. – Bratislava : Právnická fakulta, 2012 – 167 s. ISBN 978-80-7160-327-6.

[45] ĽALÍK, T.: Úvod do problematiky ľudských práv. In: Ústavné právo. - ISBN 978-80-8168-511-8. - Bratislava : Wolters Kluwer, 2016. S. 285.

[46] MACENAINTE, M. – KOSTA, E.: Consent for processing children´s personal data in the EU: following in US footsteps? In Information & Communications Technology Law, 26:2, s. 145 – 197 alebo BUITELAAR, J.C.: Child´s Best Interest and Informational Self-Determination: What the GDPR can learn from children´s rights. In International Data Privacy Law, 2018, Vol. 8, No. 4, s. 293 – 308.

[47] MAGNUSKA, K.: A mystery shopper is not always useful in dismissing an employee. Dostupné na:

[48] MATES, P. – JANEČKOVÁ, E. – BARTÍK, V.: Ochrana osobních údajů. Praha : Leges, 2012, s. 82.

[49] MATES, P.: Ochrana soukromí v správním právu. 2. aktualizované a podstatně přepracované vydání, Linde, Praha, s. 149-150.

[50] MESARČIK, M. Ochrana osobných údajov. In ANDRAŠKO, J. – HORVAT, M. – MESARČÍK, M.: Vybrané kapitoly práva informačných technológií I. Bratislava: Univerzita Komenského v Bratislave, 2019.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[51] MIČUDOVÁ, T. Zákon o oznamovaní protispoločenskej činnosti. Komentár. 1. vyd. Bratislava: Wolters Kluwer, 2016, s. 45–47.

[52] MORÁVEK, J. in PICHRT, J. a kol.: Zákoník práce. Zákon o kolektivním vyjednávání. Praktický komentář. Praha: Wolters Kluwer, 2017.

[53] MORÁVEK, J.: Možnosti monitorování zaměstnanců na pracovišti v právním řádu České republiky. In: BARANCOVÁ, H. a kol. Monitorovanie zamestnancov a právo na súkromný život, Bratislava: Sprint dva, 2010, str. 36 a nasl., ISBN: ISBN 978-80-89393-43-5.

[54] MORÁVEK, J.: Několik úvah nad (ne)možnou novelizací Zákoníku práce souvislosti s právní úpravou chráneného oznamování škodlivých jednání, str. 55. In: Acta Universitatis Carolinae – Iuridica 4, 2016, 49 – 71 s., ISSN: ISSN 0323-0619.

[55] MORÁVEK, J.: O vhodnosti a o nevhodnosti novelizace Zákoníku práce. In GREGOROVÁ, Z. (ed.): Pracovní právo 2016 : Zákoník práce v novelizaci, důchodová reforma v akci Brno : Masarykova univerzita, 2017, s. 50.

[56] MORÁVEK, J.: Ochrana osobních údaju v pracovněprávních vztazích. 1. Vyd. Praha: Wolters Kluwer ČR, 2013., 436 s., ISBN: 978-80-7478-139-1.

[57] MORÁVEK, J.: Změny tradičných institutů a institucí v době 4.0 a jejich reflexe v rámci pracovnéprávn ílegislativy. Str. 43, In: BARANCOVÁ, H., OLŠOVSKÁ, A. (eds.): Priemysel 4.0 a pracovné podmienky. Praha: Leges, 2018, 128 s., ISBN: 978-80-7502-312-4.

[58] OLŠOVSKÁ, A.: Skončenie pracovného pomeru. Bratislava: Wolters Kluwer, 2015, str. 83, ISBN: 978-80-7552-001-2.

[59] PAAL, P. - PAULY, D.A.: Datenschutz-Grundverordnung Bundesdatenschutzgesetz. 2. Auflage. München : C.H.BECK, 2018.

[60] PICHRT. J., MORÁVEK, J.: Whistleblowing. Právo pro podnikání a zaměstnání, Praha: Comenius Print, č.: 7-8/2009, str. 19, ISSN: 1801-6014.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[61] PICHRT. J.: Několik poznámek k whistleblowingu, loajalitě zaměstnance a k legislativním návrhům in PICHRT, J. (ed.) Whistleblowing. Praha: Wolters Kluwer ČR, 2013, str. 12 a nasl., ISBN: ISBN 978-807478-393-7.

[62] PORUBAN, A. Vybrané pracovnoprávne aspekty ochrany oznamovateľov na Slovensku, s. 27. In: PICHRT, J., MORÁVEK, J. (eds.) Whistleblowing – minulost, přítomnost, budoucnost. Praha: Wolters Kluwer ČR, 2020, 140 s.

[63] PORUBAN, A.: Pracovný posudok, potvrdenie o zamestnaní a osobný spis zamestnanca. In Súkromné právo, 2/2018, s. 74-80.

[64] PRÍBELSKÝ, P., LIŠIAK, P., ČERNÁKOVÁ, J.: Ochrana súkromia na pracovisku z pohľadu ústavného práva. Plzeň: Aleš Čeněk, 2014, str. 14, ISBN: 978-80-7380-476-3.

[65] PRUSÁK, J. Teória práva. 2. vyd. Bratislava: Vydavateľské oddelenie PF UK, 2001. ISBN 80-7160-146-2, 188 s.

[66] RUMANA, I., ŠINGLIAROVÁ, I. (eds.) Judikatúra vo veciach slobodného prístupu k informáciám. Bratislava : Wolter Kluwer, 2014, s. 15.

[67] RYBÁROVÁ, M. in BARANCOVÁ, H. a kol.: Zákonník práce : komentár. 2. vyd. Bratislava : C.H. Beck, 2019, s. 748.

[68] SISKOVIČOVÁ, K.: Ochrana súkromia a osobných údajov zamestnanca, 1. vyd., Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, ISBN: 978-80-8082-932-2.

[69] SVÁK, J.: Zásady a tendencie práva na súkromie. Justičná revue, 52, 2000, č. 11, s. 1199 – 1215.

[70] SZCZECHOWICZ K., ORŁOWSKA- ZIELIŃSKA B.: Chosen aspects of the protection of private communication in legal systems and the influence of the European Court of Human Rights jurisdiction on their formation by the application of procedural telephone interception, Studia Prawnoustrojowe, Wydawnictwo UWM, Olsztyn 2012, 318 s.

[71] ŠVEC, M. - TOMAN, J. a kol.: Zákonník práce. Zákon o kolektívnom vyjednávaní ; komentár zväzok 1 čl. 1 až § 176 Zákonníka práce. Bratislava: Wolters Kluwer, 2019. 1479 s.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[72] ŠVEC, M. a kol.: Kultúra sveta práce. Závislá práca a dohody o prácach vykonávaných mimo pracovného pomeru. Bratislava: Fridrich Ebert Stiftung, 2012, str. 22, ISBN: 978-80-89149-23-0.

[73] ŠVEC, M., VALENTOVÁ, T.: Ochrana osobných údajov v pracovnoprávnych vzťahoch. 1. vyd. Bratislava:

[74] TODOLÍ-SIGNES, A.: Spanish riders law and the right to be informed about the algorithm.

[75] TOMAN, J: Individuálne pracovné právo. Všeobecné ustanovenia a pracovná zmluva. Bratislava: Friedrich Ebert Stifung, 2014, str. 155, ISBN: 978-80-89149-42-4.

[76] TOSONI, L. The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation, International Data Privacy Law, 2021, Vol. 11, No. 2 145-162

[77] VALENTOVÁ, T. – BIRNSTEIN, M. – GOLAIS, J.: GDPR/Všeobecné nariadenie o ochrane osobných údajov. Zákon o ochrane osobných údajov. Praktický komentár. Bratislava: Wolters Kluwer, 2018, s. 442.

[78] VAN ALSENOY, Brendan: Liability under EU Data Protection Law. In 7 (2016) JIPITEC 271.

[79] VARGA, V.: Mzda ako osobný údaj. In: Právne nástroje odmeňovania v 21. storočí. Bratislava : Friedrich Ebert Stiftung, 2017. s. 70.

[80] VARGA, V.: Náhrada škody a nemajetkovej ujmy dotknutej osoby pri úniku jej (nielen) zdravotných údajov z cloudu. In: Starostlivosť o zdravie zamestnancov. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2018, s. 346.

[81] VYSOKAJOVÁ, M. – KAHLE, B. – DOLEŽÍLEK, J.: Zákoník práce s komentářem. Praha: ASPl, a. s. 2007, s. 317.

[82] WAGNEROVÁ, E., ŠIMÍČEK, V., LANGÁŠEK, T., POSPÍŠIL, I. a kol. Listina základních práv a svobod. Komentář. Praha: Wolters Kluwer, 2012, str. 27 a nasl.

[83] WILFLING P. Zákon o slobodnom prístupe k informáciám. Komentár, problémy z praxe, rozhodnutia súdov. Pezinok : Via Iuris, 2012.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[84] ZIMEN, O.: Biometrické dochádzkové systémy a ich problémy s reguláciou ochrany osobných údajov. Dostupné na: https://www.pravnenoviny.sk/biometricke-dochadzkove-systemy-a-ich-problemy-s-regulaciou-ochrany-osobnych-udajov. (Navštívené dňa 27.10.2023, 18:50 hod.)

[85] ŽUĽOVÁ, J. – ŠVEC, M.: GDPR a ochrana záujmov zamestnanca. Bratislava : Friedrich Ebert Stiftung, 2018, s. 96.

Judikatúra:

[1] Rozhodnutie ESĽP v právnej veci Klass z roku 1978.

[2] Rozhodnutie Krajského súdu v Bratislave sp. zn. 19 S 216/02 zo dňa 14. novembra 2002.

[3] Rozhodnutie Landesarbeitsgericht Baden-Württemberg z 20.12.2018. sp. zn. 17 Sa 11/18.

[4] Rozhodnutie Najvyššieho správneho súdu Poľskej republiky sp. zn.: I OSK 249/09.

[5] Rozhodnutie Najvyššieho súdu ČR, sp.zn.: 21 Cdo 4596/2014 zo dňa 26.11.2015.

[6] Rozhodnutie Najvyššieho súdu SR sp. zn. 2Sžo/190/2008.

[7] Rozhodnutie Najvyššieho súdu SR sp. zn. 3 Sži 29/2013; citované podľa Ruamana, I., Šingliarová, I. (eds.) Judikatúra vo veciach slobodného prístupu k informáciám. Bratislava : Wolter Kluwer, 2014, s. 20.

[8] Rozhodnutie Najvyššieho súdu SR sp. zn. 3Sž/16/2004 z 8. apríla 2005.

[9] Rozhodnutie Najvyššieho súdu SR sp. zn. 6Sži/27/2013 z 24. septembra 2014.

[10] Rozhodnutie NS ČR, sp.zn.: 21 Cdo 4596/2014 zo dňa 26.11.2015.

[11] Rozhodnutie Ústavného súdu Slovenskej republiky, sp. zn. IV. ÚS 254/2018-10.

[12] Rozhodnutie Ústavného súdu SR sp. zn. III. ÚS 96/2010; citované podľa Rumana, I., Šingliarová, I. (eds.) Judikatúra vo veciach slobodného prístupu k informáciám. Bratislava : Wolter Kluwer, 2014, s. 28.

[13] Rozhodnutie Ústavného súdu SR, sp. zn.: I. ÚS 274/05

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[14] Rozhodnutie Ústavného súdu SR, sp. zn.: I. ÚS 274/05.

[15] Rozhodnutie Ústavného súdu SR, sp. zn.: II. ÚS 280/09.

[16] Rozsudky Z proti Fínsku, 1997, § 96; C.C. proti Španielsku, 2009, § 33; P. a S. proti Poľsku, 2012, § 128; Avilkina a ostatní proti Rusku, 2013, § 45; Y. proti Turecku (odm.), 2015, § 65; Y. G. proti Rusku, 2022, § 45).

[17] Rozsudky: C-342/12, Worten – Equipamentos para o Lar SA/Autoridade para as Condições de Trabalho (ACT), 30. mája 2013.

[18] Rozsudky: Spojené veci C-465/00, C-138/01 a C-139/01, Rechnungshof/Österreichischer Rundfunk a i. a Christa Neukomm a Joseph Lauermann/Österreichischer Rundfunk, 20. mája 2003.

[19] Rozsudok C 13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme."

[20] Rozsudok ESĽP v právnej veci (Klass / Nemecko) z roku 1978.

[21] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Barbulescu v. Rumunsko, žiadosť č. 61496/08

[22] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Barbulescu v. Rumunsko, žiadosť č. 61496/08

[23] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Fernández Martínez v. Španielsko, žiadosť č. 56030/07

[24] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Köpke v. Nemecko, žiadosť č. 420/07

[25] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Niemetz v. Nemecko z 16.12.1992

[26] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Smirnova v. Rusko, žiadosť č. 46133/99 a 48183/99

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[27] Rozsudok Európskeho súdu pre ľudské práva v Štrasburgu, Vukota-Nojič v. Švajčiarsko, žiadosť č. 61838/10

[28] Rozsudok I. ÚS 144/2017, bod 3:

[29] Rozsudok Krajského súdu v Košiciach sp. zn. 7S/52/2014 zo 14. januára 2015.

[30] Rozsudok Najvyššieho súdu Českej republiky, sp. zn: 21Cdo 4733/2015.

[31] Rozsudok Najvyššieho súdu Slovenskej republiky, sp. zn.: 3 Cdo 134/2005.

[32] Rozsudok Najvyššieho súdu SR sp. zn. 6 Sžo 250/2008 z 25. novembra 2009.

[33] Rozsudok Najvyššieho súdu SR sp. zn. 6 Sžo 250/2008 z 25. novembra 2009.

[34] Rozsudok NS SR z 12.09.2016, sp. zn. 3Cdo/233/2015.

[35] Rozsudok SD EÚ v právnej veci Pán X/ Európska centrálna banka, C – 333-1999 zo dňa 18.10.2001.

[36] Rozsudok SD EÚ v právnej veci Stauder, C-29/69 zo dňa 12.11.1969, bod 419 odôvodnenia.

[37] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12.

[38] Rozsudok Súdneho dvora zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16.

[39] Uznesenie Krajského súdu v Bratislave sp. zn. 2S 300/12-26 z 5. decembra 2012 potvrdené rozhodnutím Najvyššieho súdu SR sp. zn. 6Sži/4/2013 z 19. marca 2014.

[40] Uznesenie Ústavného súdu SR sp. zn. III. ÚS 96/2010-14 z 9. marca 2010, s. 10.

[41] Uznesenie Ústavného súdu SR sp. zn.: II 280/09-16 zo dňa 10.09.2009.

[42] Nález Ústavného súdu Slovenskej republiky č. I. ÚS 117/2007 z dňa 4. 2. 2009

[43] Nález Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 1/09 z 19. januára 2011.

[44] Nález Ústavného súdu SR I. ÚS 33/95.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk

[45] Nález Ústavného súdu SR PL ÚS 43/95. Nález z 10. septembra 1996. Zbierka nálezov a uznesení Ústavného súdu SR 1996, s. 144).

[46] Nález Ústavného súdu SR sp. zn. II. ÚS 184/2015 zo dňa 11. novembra 2015

[47] Nález Ústavného súdu SR z 15.10.1997 sp. zn. II. ÚS 59/97. Zbierka nálezov a uznesení Ústavného súdu Slovenskej republiky 1997, s. 290-291.

[48] Nález Ústavného súdu SR, sp. zn.: 152/08.

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje.
www.esf.gov.sk www.employment.gov.sk www.ia.gov.sk