UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

ANALIZA ODLOČITVE EVROPSKEGA SODIŠČA ZA ČLOVEKOVE PRAVICE V PRIMERU BARBULESCU PROTI ROMUNIJI

Rebeka Vukovič

Ljubljana, avgust 2020

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo

ANALIZA ODLOČITVE EVROPSKEGA SODIŠČA ZA ČLOVEKOVE PRAVICE V PRIMERU BARBULESCU PROTI ROMUNIJI

Kandidatka: Rebeka Vukovič
Vpisna številka: 04160201
Študijski program: Visokošolski strokovni študijski program Uprava 1. stopnja

Mentorica: izr. prof. dr. Valentina Franca

Ljubljana, avgust 2020

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Rebeka Vukovič, študentka Visokošolskega strokovnega študijskega programa Uprava 1. stopnja, z vpisno številko 04160201, sem avtorica diplomskega dela z naslovom Analiza odločitve Evropskega sodišča za človekove pravice v primeru Barbulescu proti Romuniji.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbela, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbela, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisala v predloženem delu;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorski in sorodnih pravicah, Ur. list RS, št. 21/95), kršitev pa se sankcionira tudi z ukrepi po pravilih Univerze v Ljubljani in Fakulteto za upravo;
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za upravo;
- je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo dela v zbirki Dela FU.

Diplomsko delo je lektoriral: Ivan Cepanec, prof. slov. in zgod.

Ljubljana, 4. 8. 2020

Podpis avtorice:

POVZETEK

Osrednji del diplomskega dela predstavlja analiza primera Barbulescu proti Romuniji 61496/08 iz Evropskega sodišča za človekove pravice. Romunskega državljana Bogdana Mihaia Barbulescuja je delodajalec odpustil z delovnega mesta prodajnega inženirja, ker je ta med delovnim časom uporabljal službeno elektronsko pošto za dopisovanje v zasebne namene. Barbulescu se je po neuspešnih poskusih izpodbijanja odpovedi pogodbe o zaposlitvi na nacionalnih sodiščih pritožil na ESČP, z argumentom, da mu je bila z neutemeljenim nadzorom in vpogledom v vsebino dopisovanja s strani delodajalca, po 8. členu Evropske konvencije o človekovih pravicah kršena pravica do spoštovanja zasebnosti, doma in dopisovanja. Mali senat kršitve 8. člena EKČP ni ugotovil, ni pa dejansko presojal dopustnosti dejanj tako zaposlenega kot njegovega delodajalca. Mali senat je presojal le, če so romunska sodišča v postopkih storila vse, kar je v njihovih obveznostih, da bi ustrezno zaščitila tožnikove pravice v okviru disciplinskega postopka, katerega najstrožji ukrep je bil prenehanje delovnega razmerja. Premik se je zgodil pred Velikim senatom ESČP, ki je razsodil, da je od posameznika nemogoče popolnoma izključiti zasebno življenje, kljub temu da je na delovnem mestu, in s tem Barbulescuju priznal kršitev 8. člena EKČP. Ugotovili smo, da lahko delodajalec nadzoruje elektronsko pošto zaposlenega le, če ima za to utemeljen in zakonit razlog ter če o nadzoru zaposlene obvesti vnaprej, pri čemer lahko v vsebino zasebnih sporočil vpogleda le v izjemnih primerih, po navadi z odredbo sodišča. ESČP je s slednjim primerom postavilo državam članicam strožje kriterije pri tehtanju med interesom zaposlenega do pričakovanja zasebnosti na delovnem mestu ter delodajalčevim interesom preverjanja namembnosti službene opreme in preverjanja storilnosti zaposlenega. Doprinos diplomskega dela je predvsem oblikovati priporočila delodajalcem v zvezi z nadzorom nad službeno-komunikacijsko opremo, oziroma elektronsko pošto zaposlenih ter opozoriti na dejstvo, da je na delovnem mestu meja med službenim in zasebnim zelo tanka.

Ključne besede: Evropsko sodišče za človekove pravice, analiza sodne prakse, 8. člen EKČP, elektronska pošta, zasebnost na delovnem mestu, nadzor, analiza pravnih virov.

ABSTRACT

ANALYSIS OF THE EUROPEAN COURT OF HUMAN RIGHTS DECISION IN THE CASE OF BARBULESCU V. ROMANIA

The central part of the diploma thesis presents an analysis of the case 61496/08 Barbulescu v. Romania from the European Court of Human Rights. Romanian citizen Bogdan Mihai Barbulescu was fired from the post of sales engineer by his employer because he was using work electronic mail during business hours for personal purposes. After unsuccessful attempts to challenge the termination of employment in national courts, Barbulescu appealed to the ECtHR, arguing that his right to respect for private life, home and correspondence under the Article 8 of the European Convention on Human Rights has been violated by his employer with an unjustified control and access to the content of correspondence. The Small Chamber did not find a violation of the Article 8 of the ECHR, however, it did not in fact evaluate admissibility of actions of both the employee and his employer. The Small Chamber only evaluated whether the Romanian courts had done everything in their power during the proceedings to adequately protect the plaintiff's rights in the context of disciplinary proceedings, the most severe of which was the termination of employment. The shift happened before the Grand Chamber of the ECtHR, which ruled that it was impossible to completely exclude private life from an individual, even in the workplace, thus recognizing a violation of the Article 8 of the ECHR. We have found that an employer can control employee's electronic mail only if they have a valid and legitimate reason and if they inform the employee in advance, and can read the content of personal messages in exceptional cases, usually with a court order. With this case, the ECtHR has set stricter criteria for the Member States in weighing between employee's interest in expectation of workplace privacy and employer's interest in checking the use of office equipment and checking employee productivity. Contribution of the diploma thesis is primarily to formulate recommendations for employers regarding the control of office communication equipment and electronic mail of employers, and to underline the fact that there is a very thin line between working and private life in the workplace.

Key words: European Court of Human Rights, case law analysis, Article 8 of the ECHR, electronic mail, workplace privacy, surveillance, analysis of sources of law.

KAZALO

SEZNAM UPORABLJENIH KRATIC

EKČP	Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin
ESČP	Evropsko sodišče za človekove pravice
EU	Evropska unija
GDPR	Splošna uredba EU o varstvu osebnih podatkov
IKT	Informacijsko komunikacijska tehnologija
KZ-1	Kazenski zakonik
MOD	Mednarodna organizacija dela
OZ	Obligacijski zakonik
RS	Republika Slovenija
URS	Ustava Republike Slovenije
ZDR-1	Zakon o delovnih razmerjih
ZEKom-1	Zakon o elektronskih komunikacijah
ZVOP-1	Zakon o varstvu osebnih podatkov
ZVOP-2	predlog Zakona o varstvu osebnih podatkov

1 UVOD

Pri uporabi službene elektronske opreme za potrebe komunikacije na delovnem mestu se je težko izogniti vprašanju, ali jo zaposleni uporablja zgolj za potrebe dela ali morebiti tudi za urejanje zasebnih zadev in krajšanje delovnega časa. Slednje lahko predstavlja težave marsikateremu delodajalcu. Ustava Republike Slovenije (URS, Uradni list RS, št. od 33/91-I do 75/16 – UZ70a) delodajalcem priznava lastninsko pravico do preverjanja namembnosti službene opreme, obenem pa zaposlene ščiti s pravico do zasebnosti, katero le-ti v določeni meri pričakujejo tudi na delovnem mestu (Brajnik, 2019). S porastom tehnologije se je meja med svetovnim spletom in elektronsko pošto, ki je že nekaj časa nepogrešljiv komunikacijski pripomoček, predvsem v storitvenem sektorju še nekoliko bolj zabrisala, saj uporabnik do nje dostopa preko brskalnika, ki ga ponuja storitev interneta (Karlovšek idr., 2008, str. 60). Posebej v storitvenem sektorju je skoraj nemogoče pričakovati, da zaposleni ne bi imeli dostopa do svetovnega spleta, saj ga le-ti pri svojem delu potrebujejo tako za nemoteno poslovanje, kot za pridobivanje različnih informacij. Vendar tako kot prednosti, ki jih omogoča razvoj tehnologije, obstajajo tudi slabosti, saj lahko dostop do spleta v službenem času pomeni tudi priložnost za kratkočasenje oz. opravljanje nalog za zasebne namene, ki ne spadajo v delovno okolje (Karlovšek idr., 2008, str. 57). V Sloveniji je temeljni zakon, ki ureja področje uporabe elektronskih sredstev, Zakon o elektronskih komunikacijah (ZEKom-1, Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17), ker pa govorimo o uporabi elektronskih sredstev, ki jih zaposleni potrebujejo za potrebe dela, to področje ureja tudi Zakon o delovnih razmerjih (ZDR-1, Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS in 81/19).

Digitalizacija je po drugi strani pripomogla tudi delodajalcem, saj imajo ti na trgu vedno več možnosti načinov izvajanja nadzora nad svojimi zaposlenimi, prav tako je programska oprema, ki omogoča nadzor, vedno bolj ugodna (Brajnik, 2019). Nadzor nad internetom oziroma svetovnim spletom in elektronsko pošto, ki sta del tega, je v praksi zelo pogost, ne smemo pa pozabiti, da lahko s pretiranim nadzorom delodajalec hitro poseže v zasebnost zaposlenega, ki je s Konvencijo o varstvu človekovih pravic in temeljnih svoboščin, Zakon o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2 ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (EKČP, Uradni list RS – Mednarodne pogodbe, št. 7/94) zaščitena tudi na mednarodni ravni.

Običajno delodajalci že v internem pravilniku prepovedujejo uporabo službene opreme v zasebne namene. Če se osredotočimo na elektronsko pošto zaposlenega, je le-ta namenjena izključno nalogam, ki spadajo v opis dela, zato se predlaga ločevanje med službenimi in zasebnimi elektronskimi predali (Blanpain & Gestel, 2004). Predvsem spletna pošta (ang. Webmail), kot sta Gmail in Hotmail, je v podjetjih prisotna že nekaj časa

(Karlovšek idr., 2008, str. 60), z razponom socialnih omrežij pa je postala na delovnih mestih priljubljena tudi uporaba t. i. namenskih klepetalnikov (ang. messenger), aktualni pa so predvsem zato, ker med drugim omogočajo še hitrejšo komunikacijo med uporabniki (Brosix, 2020). Kljub temu da naj bi službena elektronska pošta vsebovala zgolj sporočila poslovne vsebine, se lahko včasih nehote, nevede bodisi tudi namenoma zgodi, da se v službenem poštnem predalu znajde tudi kakšno sporočilo z zasebno vsebino.

Delodajalci se za nadzor nad zaposlenimi z vidika pregledovanja internetne aktivnosti največkrat odločijo zaradi določenih tveganj, med katerimi je v prvi vrsti padec produktivnosti zaposlenih. Iz tega razloga nekateri delodajalci že blokirajo dostop do določenih spletnih strani, oziroma popularnih družbenih omrežij, saj se lahko na ta način nehote izda kakšna poslovna skrivnost, pomembna za poslovanje podjetja, kar pa bi ob morebitnem vdoru v račun zaposlenega predstavljalo težave za podjetje oz. delodajalca (Franca, 2010). Poleg varovanja občutljivih, oziroma zaupnih podatkov pred vdorom nepooblaščenim osebam je delodajalcem v interesu tudi preprečiti preobremenjenost strežnikov (Drozg, 2015), ki bi jo lahko povzročili različni škodljivi mehanizmi, kot so na primer računalniški virusi, verižna sporočila itd.

Delodajalec z izvajanjem nadzora nad službeno-komunikacijsko opremo dostopa do osebnih podatkov zaposlenega, ki so lahko tudi občutljive, oziroma zaupne narave. Na evropski ravni ravnanje z osebnimi podatki trenutno ureja Splošna uredba o varstvu osebnih podatkov (ang. GDPR – General Data Protection Regulation), Uredba 2016/697 Evropskega parlamenta in Sveta z dne 27. 4. 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Uradni list EU, št. 119, z dne 4. 5. 2016), ki je zavezujoča za vse države članice, v Sloveniji pa poleg URS, varstvo osebnih podatkov na tistih področjih, ki jih Uredba EU ne ureja, konkretneje določa Zakon o varstvu osebnih podatkov (ZVOP-1, Uradni list RS, št. 94/07 – uradno prečiščeno besedilo).

V diplomskem delu se osredotočamo na delodajalčev nadzor nad elektronsko pošto zaposlenega. V tem primeru se pojavijo trije interesi (Makarovič idr., 2003, str.136). Interes delodajalca, ki ima lastninsko pravico nad opremo (nad omrežji ter računalniki) in omejeno pravico do preverjanja, ali se oprema uporablja v skladu z namembnostjo. Prav tako je delodajalcu v legitimnemu interesu preprečevati in kaznovati kršitve zaposlenih, ki bi se lahko ob tem pojavile. Na drugi strani obstaja interes zaposlenega, ki si želi zasebnosti in samostojnosti, kljub temu da je na delovnem mestu, pri elektronski pošti pa se pojavlja še tretji interes, in sicer interes t. i. tretjih oseb. Te delavcu oz. zaposlenemu pošiljajo sporočila na službeni elektronski naslov iz različnih razlogov, pri tem pa ni nujno, da sploh vedo, da je le-ta služben (Makarovič idr., 2003, str. 136).

Po drugi strani lahko prekomerno nadzorovanje delavcu škoduje, saj le-ta svoje delo

opravlja pod stresom, ta pa lahko posledično negativno vpliva na njegovo produktivnost in njegovo motiviranost za opravljanje delovnih nalog (SPIRIT Slovenija, 2019). Kljub temu da delavca varuje pravica do zasebnosti, to še ne pomeni, da mu je na delovnem mestu dovoljeno prav vse, saj tako kot delodajalčeva lastninska pravica nad opremo, tudi ta pravica ni absolutna (Brajnik, 2019).

Dejstvo je, da je informacijska tehnologija vedno korak pred pravom, zato je tudi zakonodaja temu prilagojena. Z napredkom tehnologije je treba vedno znova določiti vrsto pravil, vendar potreba po ostalih pride šele po določenem času, ko dobi tehnologija še neko dodatno vrednost (Karlovšek idr., 2008, str. 10). Pomembno je, da delodajalec ta pravila pozna, jih dosledno upošteva in na pravilen način z njimi tudi seznani zaposlene.

Ko govorimo o uporabi elektronske pošte na delovnem mestu, ta torej predstavlja več interesov, zato je treba za vsak primer posebej pretehtati, ali bo v konkretnem primeru prevladal interes delodajalca, ki ima v lasti službeno opremo ali interes zaposlenega, ki ima, kljub temu da je na delovnem mestu, pravico do zasebnosti. V ospredju diplomskega dela bo analiza sodnega primera iz Evropskega sodišča za človekove pravice, kjer je prišlo do spora med zgoraj omenjenima interesoma.

Namen diplomskega dela je preučiti dopustnost delodajalčevega posega v zasebnost posameznika z vidika vpogleda v službeno-komunikacijsko opremo na delovnem mestu.

Cilji diplomskega dela so analiza mednarodnih in nacionalnih pravnih virov, analiza sodbe Barbulescu proti Romuniji iz Evropskega sodišča za človekove pravice ter oblikovanje priporočil slovenskim delodajalcem glede nadzora elektronske pošte zaposlenega.

V sklopu pisanja diplomskega dela si na osnovi analiziranih mednarodnih in nacionalnih pravnih virov, preučevane strokovne literature in člankov ter primera iz sodne prakse postavimo dve raziskovalni vprašanji.

V prvem raziskovalnem vprašanju ugotavljamo, kako lahko delodajalec nadzoruje elektronsko pošto zaposlenega? Zanima nas, katere pogoje mora delodajalec upoštevati in izpolnjevati, da je nadzor nad vsebino elektronske pošte zaposlenega, ki velja za precej invazivno metodo posega v zasebnost, sploh dovoljen.

V drugem raziskovalnem vprašanju, ki se glasi: *Katera pravila bodo morala nacionalna sodišča v primeru spora med delavcem in delodajalcem na podlagi sodbe* Barbulescu proti Romuniji *upoštevati in kakšna priporočila so se izoblikovala na podlagi tega primera v zvezi z ravnanjem z elektronsko pošto na delovnem mestu?,* se osredotočamo na pomen sodbe Barbulescu proti Romuniji za nadaljnje urejanje odnosov med delavci in delodajalci na področju delodajalčevega nadzora službeno-komunikacijske opreme delavca.

Pri izdelavi diplomskega dela uporabimo v uvodnem poglavju deskriptivno metodo za opis problematike nadzora službeno-komunikacijske opreme zaposlenega.

V drugem poglavju uporabimo metodo analize sekundarnih podatkov, torej mednarodnih in nacionalnih pravnih virov, s katero preučimo pravne vire, kot so EKČP, Direktiva 95/46/ES Evropskega parlamenta in Sveta, z dne 24. 10. 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takih podatkov (Uradni list EU, št. 182 z dne 23.11.1995), Kodeks o varstvu osebnih podatkov delavcev Mednarodne organizacije dela, URS, ZDR-1, ZVOP-1 ter ZEKom-1.

V tretjem poglavju analiziramo odločitev Evropskega sodišča za človekove pravice v primeru Barbulescu proti Romuniji, kjer predstavimo dejansko stanje primera, odločitev malega senata in odklonilno ločeno mnenje sodnika, odločitev Velikega senata, skupna odklonilna mnenja sodnikov ter pomen sodbe v evropskem prostoru.

V četrtem poglavju z metodo sinteze ugotovimo, kaj slednja sodba pomeni za nadaljnje urejanje odnosov med delavci in delodajalci na področju delodajalčevega nadzora službeno-komunikacijske opreme zaposlenega. Na tej podlagi predstavimo priporočila delodajalcem v zvezi z ravnanjem z elektronsko pošto zaposlenih ter predstavimo smernice, ki jih morajo nacionalna sodišča upoštevati, ko bodo tehtala med interesom zaposlenega in delodajalca.

Zadnje poglavje predstavlja zaključek, namenjen strnjeni predstavitvi spoznanj in razmišljanj.

2 ANALIZA PRAVNIH VIROV

Pravo narekuje subjektom ravnanje po vnaprej predpisanih pravilih, obenem pa poseže tudi tja, kjer bi lahko prišlo do kolizije dveh nasprotujočih si interesov in ob tem ogrozilo bodisi splošno družbeno ravnovesje ali temeljne človekove pravice. Formalni pravni viri določajo splošna in abstraktna pravna pravila, ki so temelj za strukturiranje konkretnih, oziroma posamičnih pravnih aktov, po katerih posameznike zavezujemo k točno določenemu ravnanju v družbi (Štampar, 2019). Kljub temu da je Ustava izhodiščni in najpomembnejši pravni vir posamezne države, ki obenem predstavlja temelj za oblikovanje zakonskih in podzakonskih predpisov, mednarodni pravni viri predstavljajo pomemben del pravnega sistema držav, saj mora biti nacionalna zakonodaja v skladu z veljavnimi načeli mednarodnega prava in mednarodnimi pogodbami, ki državo obvezujejo. Sklop mednarodnih pravnih virov, ki se nanašajo na koncept pričakovane zasebnosti, varstva osebnih podatkov in delodajalčevega nadzora nad elektronskimi sredstvi zaposlenega, je obširen, zato v točki 2.1 predstavimo nekatere ključne, oziroma temeljne mednarodne dokumente, ki se nanašajo na slednjo tematiko, v točki 2.2 pa predstavimo določbe, ki jih vsebuje slovenska zakonodaja.

2.1 MEDNARODNI PRAVNI VIRI

EKČP se je razvila po Splošni deklaraciji o človekovih pravicah in Ameriški deklaraciji o človekovih pravicah in dolžnostih. Njen začetek sega v leto 1948, ko je Evropski kongres na zasedanju v Haagu sprejel resolucijo, s katero je menil, da se morajo vsi evropski demokratični narodi zavezati, da bodo spoštovali Listino o človekovih pravicah ter da se bo ustanovila posebna komisija, ki bo sestavila to listino in določila pogoje, ki jih bo morala država spoštovati, da bomo lahko govorili o njej kot o demokratični državi (Gomien, 2009, str. 15). Statut Sveta Evrope, ki je bil podpisan 5. maja 1949, je tako vseboval elemente, ki poudarjajo pomen oz. spoštovanje človekovih pravic, 8. člen pa določa tudi, da se lahko državo članico ob morebitnem nespoštovanju le-teh suspendira oz. izključi iz Sveta. Svet Evrope je malo več kot leto dni kasneje po podpisu statuta sprejel EKČP, ki jo je 4. novembra 1950 podpisalo deset držav članic, veljati pa je začela 3. septembra 1953 (Gomien, 2009, str. 15). EKČP je nastala predvsem kot odgovor na dejanja druge svetovne vojne, v prizadevanju, da se v prihodnosti tovrstna ravnanja iz strani držav članic zoper človekove pravice ne bodo več ponovila (Gogala, 2015). Sestavljena je iz Preambule, v kateri je izražen vpliv in pomen Splošne deklaracije o človekovih pravicah, določb o pravicah in temeljnih svoboščinah, določb o položaju in delovanju Evropskega sodišča za človekove pravice (ESČP) ter raznih določb, med katerimi so pogoji za ratifikacijo, ozemeljska veljavnost itd. Njeni objekti varovanja so pravica do življenja, pravica do poštenega sojenja, spoštovanje zasebnega in družinskega življenja, svoboda mišljenja, izražanja, vesti in veroizpovedi,

pravica do učinkovitega pravnega varstva, mirnega uživanja posesti ter volilna pravica. Po EKČP je med drugim prepovedano mučenje, suženjstvo, nezakonito pridržanje, diskriminacija ter smrtna kazen (Gogala, 2015). Z nastankom EKČP se je ustanovilo ESČP, katerega delovanje je nedvomno pripomoglo k ozaveščanju in varovanju pravice do zasebnosti, katere uporabo v praksi še danes na novo interpretira, dopolnjuje in izboljšuje, v preteklosti pa je že izreklo sankcije državam, ki niso imele v zakonodaji urejene pravice do zasebnosti (Karlovšek idr., 2008). Sodbe Velikega senata ESČP so za države članice zavezujoče, sprejetje ukrepov za odpravljanje in preprečevanje kršitev v bodoče s strani posameznih držav članic pa nadzoruje Odbor ministrov Sveta Evrope (Ministrstvo za pravosodje, 2019).

EKČP je postala prvi mednarodni dokument, ki se je zavzemal za zaščito civilnih in političnih pravic tako na nacionalni ravni držav članic, kot z vidika pravno zavezujočih pogodb za visoke pogodbenice (Gomien, 2009, str. 16). Države podpisnice ji v nacionalnem pravnem redu pripisujejo različne pomene, kjer ima le-ta lahko moč Ustave ali moč zakona, prav tako se države podpisnice med seboj razlikujejo po samem zagotavljanju obveznosti spoštovanja pravic in svoboščin (Gogala, 2015). Republika Slovenija je EKČP ratificirala 31. maja 1994, z začetkom veljave 28. junija 1994 pa je EKČP za Slovenijo postala tudi zavezujoča.

Po prvi točki 8. člena EKČP ima vsak posameznik pravico uživati zasebno in družinsko življenje, si ustvariti dom in svobodno dopisovati, brez poseganja države. Ta je dolžna spoštovati in varovati omenjene objekte pravice. Zasebno življenje se nanaša na posameznikove odnose v družbi, osebna stanja, ki so zgolj v njegovi domeni in niso dolžna biti razkrita drugim osebam. Posameznik ima pravico do svobodnega ustvarjanja družine in varovanja doma, prav tako ima pravico do pisnega komuniciranja s komerkoli želi, s tem, da je vsebina dopisovanja znana le osebi, s katero si le-ta si dopisuje.

Država lahko v omenjene pravice poseže zgolj, če za to obstaja utemeljen razlog. Ti razlogi so določeni z zakonom in so nujni za zaščito državne ali javne varnosti, stabilnega ekonomskega stanja države ali z namenom preprečevanja kaznivega dejanja v dobrobit zdravja, morale ter zaščite pravic in osebnih svoboščin drugih ljudi (2. točka 8. člena EKČP).

S pravico do spoštovanja dopisovanja, ki je predmet prvega odstavka tega člena, se je ESČP prvič seznanilo v primeru Klass proti Zvezni republiki Nemčiji, zoper Zakon o omejevanju pisne, poštne in telekomunikacijske skrivnosti, imenovan »G-10« (Das Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisse, z dne 26. 6. 2001). Zakon je v nemški Ustavi (Grundgesetz) pooblaščenim državnim organom določal tajno nadzorstvo nad korespondenco oz. dopisovanjem, kar je zajemalo tudi branje pisemskih sporočil, prisluškovanje in snemanje telefonskih pogovorov. Sodišče je v slednjem primeru odločilo, da je tajni nadzor nad dopisovanjem v sodobni družbi zakonit in nujen za zagotavljanje nacionalne varnosti in preprečitve zločinov in kriminala, zato je pritožbo

zavrnilo (Armič, 2013). Čeprav v slednjem primeru do ugotovitve kršitve 8. člena konvencije o človekovih pravicah ni prišlo, je bil že sam postopek zelo pomemben za nadaljnjo sodno prakso, saj se je tukaj sodišče prvič ukvarjalo s pojmom pravica do dopisovanja (Lampe, 2004, str. 223). Sodišče je v slednjem primeru prav tako prepoznalo, da nadzor, določen z zakonom, zoper katerega so se pritožniki pritožili, ni bil najbolj primeren ter da bi bilo treba vzpostaviti sodni nadzor nad izvajanjem takšnih ukrepov, saj lahko na tem področju hitro pride do zlorab (Armič, 2013).

V zvezi z 8. členom EKČP se je ESČP v svoji sodni praksi večkrat srečalo tudi s področjem kršitev, ki se nanašajo na varstvo osebnih podatkov. S tem namenom je Svet Evrope že leta 1981 sprejel Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, Zakon o ratifikaciji konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Uradni list RS – Mednarodne pogodbe, št. 3/94 in Uradni list RS, št. 86/04 – ZVOP-1), ki je služila kot temelj pri oblikovanju nadaljnjih sodnih precedensov skozi leta (Lampe, 2004, str. 211).

Direktive predstavljajo sekundarne pravne vire EU, ki so lahko naslovljene na eno ali več držav članic; za implementacijo, oziroma prenos v pravni sistem države pa je največkrat potreben poseben pravni akt (Služba Vlade Republike Slovenije za zakonodajo, 2018). Direktive morajo doseči svoj cilj oz. namen, države pa lahko pri sami izvedbi le-tega uporabijo različne ukrepe in metode, pri čemer morajo upoštevati prenos v svojo zakonodajo pred potekom roka, ki je po navadi dve leti. Če države tega ne uredijo pravočasno, gre za kršitev prava EU, kar pomeni, da lahko Komisija sproži kazenski postopek zoper državo članico. Bistvo direktive je vpeljati močnejše varstvo pravic na določenem zakonodajnem področju, vendar le-ta državam članicam dopušča prosto presojo pri morebitni uvedbi še strožjih ukrepov zaščite pravic (Evropska komisija, b. d.). Direktive, ki so se nanašale na koncept zasebnosti, so bile sprejete z namenom, da bi se po vseh državah članicah poenotila zakonodaja varstva zasebnosti (Kovačič, 2006, str. 78) Leta 1995 je bila tako sprejeta Direktiva 95/46/ES. Nekoliko kasneje sta varstvo zasebnosti, ki se nanaša na elektronske komunikacije in telekomunikacije, konkretneje opredelili Direktiva 97/66/ES Evropskega parlamenta in Sveta z dne 15. 12. 1997 o zasebnosti telekomunikacij (Uradni list EU, št. 108, z dne 24. 4. 2002) ter Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. 7. 2002 o zasebnosti in elektronskih komunikacijah (Uradni list EU, št. 201/37, z dne 31. 7. 2002) (Kovačič, 2006, str. 82). Direktiva 95/46/ES je zavezujoča za vse države članice, neposredno pa se nanaša tudi na nadzorovanje elektronske pošte in uporabe interneta, saj pri tem delodajalec upravlja z osebnimi podatki zaposlenega (Zupančič, 2015). Direktivo je z dnem 27. 4. 2016 razveljavila Uredba GDPR. Za razliko od direktiv, ki morajo biti za svojo veljavnost implementirane v pravni red držav članic, na katere so naslovljene, imajo uredbe EU v celoti zavezujočo moč za vse države članice, v veljavnost pa vstopijo takoj po sprejetju ne glede na zakonodajo posamezne države članice (Evropska komisija, b. d.). Uredba GDPR

se uporablja od 25. 5. 2018, državam članicam pa je strožje in poenoteno zapovedala ravnanje z osebnimi podatki in predvsem uredila lažji dostop posameznikov do osebnih podatkov, strožje določila pogoje nadzora nad osebnimi podatki ter še bolj uredila varstvo pravic posameznikov pri obdelavi podatkov. Uredba med drugim posamezniku prinaša pravico biti obveščen zoper obdelave osebnih podatkov, ki se navezujejo nanj, posameznik ima prav tako pravico dostopa do osebnih podatkov, ki se obdelujejo v zvezi z njim, pravico do pozabe, kjer se, če za obdelavo ni več potrebe, podatki izbrišejo (ne zgolj anonimizirajo), pravico do ugovora obdelave osebnih podatkov, če za to obstaja utemeljen razlog itd. (Jamšek, 2018).

Po direktivi 95/46/ES morajo države članice pri obdelavi osebnih podatkov ščititi temeljne pravice posameznikov in pri tem upoštevati njihovo zasebnost (prvi odstavek 1. člena).

Osebni podatek je vsako dejstvo, vsebina, ki določa posamezno fizično osebo, bodisi se nanjo nanaša in zanjo velja. Prav zaradi teh osebnih podatkov se posamezniki med seboj bolj ali manj, vendar bistveno razlikujejo (2. a člen).

V 6. členu države članice določijo, da morajo biti osebni podatki obdelani v skladu z zakonom in biti pridobljeni na način, ki je pravičen (podatki ne smejo biti prirejeni, izbrisani, nestrokovno obdelani). Osebni podatki se lahko zbirajo samo za točno določene in legitimne namene, pri čemer se podatkov ne sme naprej obdelovati za neutemeljene ali nezakonite namene. Za posamezen namen obdelave lahko pridobimo le podatke, ki jih izrecno predvidevata načrt in cilj obdelave, torej le toliko, kolikor jih resnično potrebujemo. Podatki morajo biti točni, ne prirejeni ter aktualni, ne zastareli. Obenem je treba vse netočne, nepravilne ali pomanjkljive podatke ustrezno popraviti in dopolniti. Podatki se morajo hraniti le toliko časa, dokler jih upravljalec, oziroma obdelovalec potrebuje pri svojem delu.

Obdelava osebnih podatkov posameznika je dovoljena le v primerih, ko se posameznik s tem strinja in obenem podeli obdelovalcu, oziroma upravljalcu svoje dovoljenje. Obdelava osebnih podatkov se prav tako dovoli, če gre za podatke, pomembne za izvajanje pogodb, v katerih nastopa stranka, na katero se podatki nanašajo in so le-ti pomembni za samo izvajanje obveznosti iz le-te. Za samo obdelavo podatkov mora obstajati tudi zakonska podlaga ter izjemni primeri, ko se morajo podatki posameznika obdelovati zaradi varstva njegovih življenjskih interesov. Obdelava osebnih podatkov je dopustna tudi v primerih, ko gre za opravljanje nalog javnega interesa ali javne oblasti ter če je potrebna zaradi zakonitih in prevladujočih interesov tretje stranke, vendar ne na račun temeljnih človekovih pravic. Prav tako se obdelava osebnih podatkov ne izvaja, če posameznik v zvezi z obdelavo zahteva varstvo (7. člen).

V primeru kršitve pravic v zvezi z nacionalno zakonodajo ima vsak posameznik, na katerega so se obdelovani podatki nanašali, možnost pravnega varstva na sodišču (22. člen). Države

članice poskrbijo, da je vsakem posamezniku, kateremu so bile kratene pravice v poteku nezakonite obdelave podatkov ali katerega koli dejanja, ki je v neskladju s to direktivo, dana možnost terjanja odškodnine od upravljalca (23. člen). Države članice sprejmejo ustrezne ukrepe za izpolnitev določb direktive ter v primeru kršitev določijo sankcije (24. člen)

Po 29. členu direktive se je ustanovila Delovna skupina za varstvo posameznikov pri obdelavi osebnih podatkov, katere naloge so preučevanje vprašanj v zvezi z uporabo nacionalnih predpisov, svetovanje in podajanje mnenja Komisiji ter predlaganje sprememb in dodatnih ukrepov z namenom dodatne zaščite pravic posameznikov pri avtomatski obdelavi podatkov. Delovno skupino sestavljajo predstavniki držav članic EU, v Sloveniji to nalogo opravlja informacijski pooblaščenec. Vsa priporočila, ki jih sprejme Delovna skupina, temeljijo na direktivi 95/46/ES, države članice pa lahko svojo zakonsko podlago uredijo še nekoliko strožje (Karlovšek idr., 2008, str. 135).

29. maja 2002 je bil s strani Delovne skupine izdan delovni dokument o nadzoru elektronskih komunikacij na delovnem mestu. Z njegovo vzpostavitvijo je EU dobila prva konkretna priporočila glede upravičenega nadzorovanja elektronskih komunikacij zaposlenih na delovnem mestu (Zupančič, 2015). V njem so se prvič pojavila vprašanja v zvezi z samo transparentnostjo nadzora, kar pomeni, da mora biti vsak nadzor predviden in izveden na odkrit način, prav tako morajo biti sprejeti ukrepi nadzora ravno prav ostri oziroma nujni za dosego namena. Zbiranje podatkov o ljudeh je posebej občutljivo, zato moramo skrbno pretehtati, katere ter koliko podatkov bomo zbrali, kako jih bomo pridobili ter kdo jih bo pridobil, da bodo obdelani na način, ki bo delavcem pravičen.

Delovna skupina priporoča delodajalcem, da zaposlenim zagotovijo dva elektronska naslova. Enega namenjenega zgolj za poslovne oz. službene namene, kjer je nadzor dovoljen v skladu z določenimi omejitvami, ter drugega, namenjenega samo zasebni rabi, kjer se lahko nadzor izvaja le v izjemnih primerih, če je to potrebno za zagotavljanje varnosti ali preprečevanje in ugotavljanje kaznivih dejanj.

Prav tako naj bi se pri elektronski pošti nadzirali le prometni podatki, oziroma čas komuniciranja in ne vsebina. Delovni dokument dopušča poseg v elektronski poštni predal zaposlenega, če je ta odsoten z delovnega mesta, v primeru, da se s tem zagotavlja nemoteno poslovanje (npr. če ni zagotovljen avtomatski odzivnik ali avtomatsko posredovanje sporočil). Med drugim delovni dokument poudarja tudi dejstvo, da si delodajalec z nadzorom bolj kot kaznovati zaposlenega, želi preprečiti kaznivo dejanje s strani delavca, še preden je le-to storjeno.

Mednarodna organizacija dela (MOD) oz. International Labour Organization je najstarejša organizacija Združenih narodov. S svojo ustanovitvijo si prizadeva za pravičnejši socialni status in položaj delavcev. V njeni pristojnosti je predvsem izboljšanje delovnih pogojev

delavcev in njihovih življenjskih standardov. Sestavljajo jo tri telesa: Mednarodna (ministrska) konferenca dela, izvršilni odbor in mednarodni sekretariat za delo. Države članice se vsako leto junija sestanejo v Ženevi na Mednarodni konferenci dela (Ministrstvo za zunanje zadeve RS, 2015). Tam se diskutirajo ključna socialna in delovna vprašanja, njen temeljni namen pa je določiti mednarodne delovne standarde oz. delovne pogoje (ILO, 2020). Posamezno državo članico zastopata najmanj dva vladna predstavnika ter po en predstavnik delodajalcev in delojemalcev. Organizacija šteje 183 članic, med njimi je od leta 1992 tudi Slovenija (Ministrstvo za zunanje zadeve RS, 2015).

Kodeks o varstvu osebnih podatkov delavcev je MOD sprejela leta 1997 z namenom postavitve smernic glede varstva osebnih podatkov v delovnem razmerju, ki za države članice sicer ni zavezujoč. Že ob prvih pojavih nadzora je tako stopila v bran delavcem s stališčem, da interesi delodajalcev ne smejo poseči v njihovo pravico do zasebnosti (Zupančič, 2015). Člen 5.13 kodeksa, kjer so zapisana splošna načela, določa, da se delavci ne smejo odpovedati svoji pravici do zasebnosti. Če se osredotočimo na delodajalčev nadzor nad delavcem, je v členu 3.3 kodeksa določeno, da se pod nadzor šteje uporaba računalnikov, kamer, video opreme, zvočnih naprav, telefonov ter drugih naprav, ki omogočajo pregled nad identiteto in lokacijo.

V členu 6.14 je določeno, da morajo biti delavci vnaprej seznanjeni z namenom, časom in metodo, s katero bodo nadzorovani, pri tem pa mora delodajalec izbrati čim manj invaziven ukrep, s katerim je možno doseči zastavljen cilj. Obstajajo tudi izjeme, kjer se skrivni nadzor lahko izvaja le v primeru, da je v interesu nacionalne zakonodaje, če obstaja sum kaznivega dejanja ali, če gre za varovanje osebnega zdravja in intelektualne lastnine.

Člen 11.1 določa, da morajo biti delavci vedno obveščeni, ko se zbirajo njihovi osebni podatki. Delodajalci imajo v primeru, ko gre za preiskavo, delavcu pravico odreči vpogled v njihovo kartoteko podatkov, če bi lahko to ogrozilo nadaljnji potek le-te (člen 11.8). Člen tudi določa, da se pred koncem preiskave v zvezi z osebnimi podatki ne bo odločalo o obstoju delovnega razmerja, dokler ne bo imel delavec dostopa do obdelovanih podatkov.

EKČP je v mednarodnem prostoru nedvomno uveljavila pomemben pravni standard varovanja posameznikovega pričakovanega koncepta zasebnosti, katerega predmet varovanja so dom, družina, dopisovanje in zasebno življenje. Vsi ti štirje varovani objekti pravice do zasebnosti se med seboj razlikujejo, obenem pa se na nek način prekrivajo in dopolnjujejo (Lampe, 2004). Predvsem ESČP predstavlja pomemben institut varovanja te pravice v praksi, saj se lahko po 34. členu EKČP vsaka oseba, ki meni, da ji je bila s strani države članice kršena pravica po EKČP, pritoži zoper državo, vendar je pred tem potrebno izčrpanje vseh domačih pravnih sredstev (35. člen EKČP), torej pritožb na nacionalnih sodiščih, sicer se zgodi, da sodišče pogosto pritožbo zavrne kot neutemeljeno. ESČP se, ko v konkretnem primeru odloča o tem, ali je bila pravica do zasebnosti posamezniku kršena,

najprej sprašuje, če je v konkretnem primeru 8. člen EKČP res uporabljen oz. če so bili posameznikovi očitki o kršitvi dejansko predmet varovanja po EKČP (European Court of Human Rights, 2019). Če se izkaže potreba po nadaljnji obravnavi, sodišče ugotavlja, ali je bila tožnikova pravica do zasebnosti dejansko kršena s strani države članice ali pa je kršitev pravice nastala s tem, ko država tožniku ni zagotovila ustrezne pravne zaščite te pravice. V prvem primeru govorimo o negativni obveznosti države članice, v drugem pa o njeni pozitivni obveznosti (Brdnik, 2016). Države članice morajo za izpolnjevanje svojih pozitivnih obveznosti vzpostaviti različne ukrepe, s katerimi so dolžne pravicam zagotoviti ustrezno pravno varstvo, kar obenem predstavlja tudi politično odgovornost (Teršek, 2008). Sodišče pri svoji presoji nadalje ugotavlja, če je bil v konkretnem primeru poseg v zasebnost posameznika utemeljen na podlagi zakona, če je bil takšen ukrep sprejet z namenom doseči legitimen cilj ter ali je bil takšen poseg nujen v demokratični družbi (European Court of Human Rights, 2019). V primeru ugotovitve kršitve pravice do zasebnosti po 8. členu EKČP sodišče praviloma naloži toženi državi izplačilo zneska, ki ga mora tožniku brezpogojno poravnati, kar nadzoruje Odbor ministrov, vendar pa to samo po sebi še ne pomeni, da se s tem njena obveznost do ESČP konča. Pri izvrševanju sodbe ESČP mora država prav tako vzpostaviti prejšnje stanje in ponovno odločati v posameznih zadevah (civilnih, upravnih itd.) ter zagotoviti, da se podobne kršitve v prihodnosti ne bodo več dogajale, morebiti tudi s spremembo zakonodaje ali same Ustave (Černič, 2012). Tudi same direktive EU, ki se nanašajo na varstvo osebnih podatkov ter uporabo elektronskih sredstev, prinašajo v države članice, v kolikor so zavezujoče, posameznikom več pravic, s tem, da lahko države to področje uredijo še strožje, kot je pri nas recimo z URS strožje varovana komunikacijska zasebnost. Dejstvo, da je bila Direktiva 95/46/ES, katero je kasneje razveljavila Uredba GDPR, zavezujoča za vse države članice, nam pove, da je EU že takrat prepoznala pomen ustreznega ravnanja z osebnimi podatki ter koncept pričakovanja posameznikove zasebnosti pri obdelovanju le-teh. Po direktivi 95/46 ES je določeno, da se lahko osebni podatki obdelujejo samo ob posebnih pogojih, med katerimi mora biti izražen utemeljen in zakonit namen obdelave osebnih podatkov, pri čemer se lahko obdeluje le toliko podatkov, kot je potrebno za izpolnitev namena, posamezniki pa lahko v zvezi s tem zahtevajo tudi pravno varstvo, če menijo, da so bili njihovi osebni podatki obdelani, bodisi razkriti na namen, ki ni v skladu z direktivo. Delovna skupina je že leta 2002, ko so se nadzori nad zaposlenimi šele začeli vpeljevati, poudarila nujnost med razlikovanjem službenega in zasebnega elektronskega predala. Slednje je še posebej pomembno, saj se praviloma med službeno elektronsko pošto naj ne bi znašla sporočila zasebne narave, ker je lastnik službenega elektronskega naslova delodajalec, zaposleni pa le-tega uporabljajo za opravljanje svojega dela v njegovem imenu. Po razveljavitvi direktive 95/46/ES je Uredba GDPR državam članicam določila še višje standarde varstva osebnih podatkov, med katerim je sama privolitev v obdelavo osebnih podatkov, kjer za to ni zakonske podlage še strožje pogojena. Ob tem leži dokazno breme na strani upravljalca oz. če govorimo o delovnem

razmerju – delodajalca (Dashöfer, 2018). Slednje pomeni, da mora delodajalec v primeru, da pride do spora pred sodiščem, dokazovati, da je posameznik oz. zaposlen resnično privolil v obdelavo osebnih podatkov, zato je priporočeno, da je privolitev s strani posameznika v takem primeru podana pisno, saj je le-ta potem lažje dokazljiva. Kodeks o varstvu osebnih podatkov delavcev MOD za države članice sicer ni zavezujoč, vendar je pomemben s tega vidika, ker delodajalcem postavlja priporočila glede nadzorovanja zaposlenih in predvsem ohranja njihovo zasebnost tudi na delovnem mestu. Iz njega izhaja tudi pomembno določilo, da morajo biti zaposleni vedno obveščeni o morebitnem nadzoru in da more biti le-ta izveden na transparenten način, obenem pa priznava izjeme, v katerih je možno izvajati skrivni nadzor, vendar so te redke, kot so na primer sum na kaznivo dejanje, varnost in zdravje zaposlenih. Prav tako je poudarjeno tudi dejstvo, da si želijo delodajalci z uvajanjem nadzora, bolj kot posegati v samo zasebnost zaposlenih, preprečiti morebitna kazniva dejanja le-teh.

2.2 NACIONALNI PRAVNI VIRI

Večina evropskih držav uredi pravico do zasebnosti že z Ustavo, posamezno vrsto zasebnosti (komunikacijsko, prostorsko, informacijsko itd.) pa določi s sekundarnim varstvom, katero predstavljajo različni področni zakoni. URS zagotavlja različne pogoje za posege v zasebnost, zato je tudi varstvo zasebnosti določeno v več določbah (Karlovšek idr., 2008, str. 20). V URS so zajeta vsa najpomembnejša področja družbenega življenja, le-ta omogoča zaščito človekovih pravic, temeljnih svoboščin, ter omogoča dopolnjevanje, širjenje in razvoj ustavno pravnih norm, s čimer ohranja napredek demokracije in vladavine prava. Je živo besedilo, saj se njena vsebina vedno znova razlaga skozi različno interpretacijo (Teršek, 2018). URS je najvišji in izhodiščni splošni pravni akt, zato predstavlja tudi akt, ki ima v RS največjo pravno moč, saj le-ta predstavlja zakonsko osnovo, na kateri morajo temeljiti vsi zakonski in podzakonski predpisi (Služba Vlade Republike Slovenije za zakonodajo, 2019). V Sloveniji je najvišji organ sodne oblasti za varstvo človekovih pravic in presojo ustavnosti zakonskih določil Ustavno sodišče RS, ki je med drugim pristojno za odločanje v ustavnih pritožbah zoper temeljne človekove pravice ter presojanju, če so zakonski predpisi v skladu s samo Ustavo (Urad Vlade Republike Slovenije za komuniciranje, 2019). Ustavno sodišče RS je v zadevi U-I-25/95 z dne 27. 11. 1997 v postopku za oceno ustavnosti zakonskih določb v Kazenskem zakoniku v 32. točki odločitve argumentiralo, da je prepovedan vsak poseg v določbe, ki varujejo človekove pravice, z vidika varstva osebnega dostojanstva, osebnostnih pravic, zasebnosti in varnosti, razen tistega, ki je z izjemo dovoljen, oziroma tam, kjer pride v nasprotje z interesi drugih in ta interes v konkretnem primeru občutno prevlada (Karlovšek idr., 2008, str. 21).

V Temeljni ustavni listini o samostojnosti in neodvisnosti Republike Slovenije (Uradni list RS, št. 1/91-I in 19/91 – popr.) je zapisano, da Republika Slovenija v skladu z URS in

mednarodnimi pogodbami, ki jo obvezujejo, na svojem ozemlju varuje temeljne človekove pravice vseh oseb, brez kakršne koli oblike diskriminacije (Teršek, 2018, str. 28). Pravica do varstva zasebnosti in osebnostnih pravic je sprva določena v 35. členu, ki je hkrati tudi določba, ki zagotavlja splošno pravico do zasebnosti (Makarovič idr., 2003, str. 120). 35. člen določa, da je zagotovljena nedotakljivost človekove telesne in duševne celovitosti, njegove zasebnosti ter osebnostnih pravic. Ker je pojem zasebnosti ločen od pojma osebnostnih pravic, pomeni, da se v okviru URS pravica do zasebnosti uvršča k osebnostnim pravicam, za varstvo le-te pa je pomembna vsebina varovanega objekta, ne le določba posameznega člena (Cvetko, 1999, str. 53). Ob tem se moramo zavedati, da ni nujno, da je vsak sleherni poseg v zasebnost že protipraven, saj moramo upoštevati stopnjo in nujnost vsakega posameznega posega v zasebnost in upoštevati, kakšen je sam pomen le-tega in kdo sploh je oseba, zoper katere se posega v njegovo osebnost (Teršek, 2018, str. 173).

Za primerjavo z drugimi evropskimi državami je v Sloveniji nekoliko strožje določena komunikacijska zasebnost (Havliček, 2012). 37. člen URS namreč zagotavlja tajnost pisem in drugih občil, kjer lahko samo zakon predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem ter drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Za omejitev te pravice morajo biti izpolnjeni štirje osnovni pogoji (Karlovšek idr., 2008, str. 24):

1. poseg v pravico mora biti vnaprej določen v zakonu,
2. poseg v pravico mora biti časovno omejen,
3. poseg v pravico je dopusten, če je dovoljenje izdala sodna veja oblasti,
4. omejitev je dopustna, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.

Sam 37. člen torej poleg pisem varuje tudi druga občila, ki v tem kontekstu pomenijo vse druge možnosti načina komunikacije, kot so npr. elektronska pošta, telefonski pogovori, telefaksi itd., pri čemer se ne varuje le vsebina takšnega komuniciranja, temveč tudi vsi podatki, povezani z njo (Klemenčič, 2002). Bistveni namen tega člena je torej, da bi se preprečil neupravičen pregled vsebine sporočila tretjim osebam, kar obenem zagotavlja posamezniku svobodo o tem, komu bo sporočilo posredoval in na kakšen način. Na ta način se zagotavlja nenadzorovana komunikacija, ki posamezniku zagotavlja svobodno komunikacijo (Karlovšek idr., 2008, str. 37). Ustavno varstvo varuje tako zaseg določenega sporočila, kot samo prestrezanje le-tega, npr. nadzor elektronske pošte, čeprav gre v drugem primeru za izvajanje v nevednosti druge osebe, oziroma za poseg v komunikacijsko zasebnost na prikrit način (Klemenčič, 2002). Tudi v delovnem razmerju ima zaposlen pravico do tajnosti svojih sporočil in do svobodne komunikacije, zato mora ta člen pri postavljanju pravil in omejitev upoštevati tudi delodajalec (Karlovšek idr., 2008, str. 24).

38. člen URS določa varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov

v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor, in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi. Osebni podatki so tesno povezani s pravico do komunikacijske zasebnosti, saj so le-ti predmet varstva 38. člena, takšna ali drugačna seznanitev z njimi oz. pridobitev le-teh pa predstavlja poseg v zasebnost posameznika (Makarovič idr., 2003, str. 120).

URS po drugi strani v 33. členu zagotavlja pravico do zasebne lastnine in dedovanja. Nanjo se navezuje 67. člen, ki posamezniku priznava in varuje lastninsko pravico tako, da je zagotovljena njena gospodarska, socialna in ekološka funkcija. Predmet varstva pravice tako predstavlja vsako stvar, ki si jo posameznik posestvuje ter z njo upravlja oz. razpolaga, omejitve slednje pravice pa so lahko določene le na podlagi zakona. Lastninsko pravico nekoliko podrobneje ureja Stvarnopravni zakonik (SPZ, Uradni list RS, št. 87/02, 91/13 in 23/20), v URS pa jo uvrščamo v poglavje, ki ureja gospodarska in socialna razmerja, ne med določbe, ki varujejo temeljne človekove pravice (Karlovšek idr., 2008, str. 27)

V Sloveniji je temeljni zakon, ki ureja odnose med delavci in delodajalci, ZDR-1. Iz njega izhaja, da je zaposlen nasproti delodajalcu enakovredna stranka, vendar se v praksi pokaže, da temu ni ravno tako. Delodajalec se v delovnem razmerju izkaže za močnejšo stranko nasproti delavcu, zato ima po zakonu zelo omejene pravice, ki zadevajo varstva osebnih podatkov zaposlenih (Karlovšek idr., 2008, str. 11). Zakona, ki bi urejal vprašanje zasebnosti delavca na delovnem mestu tako na univerzalni, kot na regionalni ravni, trenutno še ni, pravica do zasebnosti, določena z URS pa vendar velja tudi na področju delovnega razmerja (Zupančič, 2015). Danes so delodajalci in delojemalci večinoma dobro seznanjeni o pravicah na delovnem mestu. K temu je nedvomno prispeval splet, kjer je poleg raznih člankov na to tematiko možno zaslediti tudi odmevne sodne primere, prav tako se s svojimi stališči in priporočili večkrat opredeljuje tudi informacijski pooblaščenec (Bečan idr., 2016, str. 257).

1. odstavek 4. člena ZDR-1 določa, da opravlja delavec delo po navodilu in nadzoru delodajalca, kjer se oseba prostovoljno vključi v organiziran delovni proces po navodilih delodajalca in v njem za plačilo nepretrgoma opravlja delo, v 2. odstavku 4. člena pa je določeno tudi, da morajo vse pogodbene stranke v delovnem razmerju spoštovati dolžnosti sklenjene z le-tem (Bečan idr., 2016, str. 37). Po 6. členu ZDR-1 je prepovedana posredna diskriminacija, o kateri bi lahko govorili tudi, ko je zaposleni na podlagi osebne okoliščine podvržen obliki delodajalčevega nadzora, ki ni utemeljen na zakonski podlagi oz. z ustaljeno sodno prakso (Feguš, b. d.). Delodajalec bi lahko v takem primeru izvajal nadzor zgolj nad določenimi zaposlenimi, bodisi zaradi predsodkov ali ''iskanja krivde'', vendar za samo izvajanje nadzora ne bi obstajali zakoniti oz. tehtni razlogi. Težava nastane tudi, ko delodajalec s svojim nadzorom bodisi namenoma ali nehote poseže v delavčevo zasebnost s tem, ko pridobi zasebne osebne podatke o zaposlenem, do katerih ni nujno upravičen

(Zupančič, 2015). Pri nadzoru službene elektronske pošte zaposlenega s strani delodajalca namreč lahko nastane problem, ker obstaja možnost, da jo zaposlen uporablja tako v službene, kot zasebne namene, v takem primeru pa je težko ločiti predmet vsebine. Po drugi strani 46. člen ZDR-1 določa, da mora delodajalec varovati in spoštovati delavčevo osebnost ter spoštovati in zaščititi njegovo zasebnost, kar pomeni, da splošno priznane osebnostne pravice nedvomno veljajo tudi na področju delovnega razmerja. Vendar je ob tem treba poudariti, da ima tudi delodajalec priznano splošno pravico do nemotenega vodenja delovnih procesov in ustreznega ukrepanja ob primerih, ko bi le-ti lahko bili ogroženi. V primerih morebitnih konfliktov je priporočeno, da poskušajo delavci in delodajalci sporazumno najti rešitve, še preden poiščejo pravno varstvo na sodiščih ali s pomočjo inšpektorjev za delo (Bečan idr., 2016, str. 256–257).

Nekoliko podrobneje varuje delavčeve osebne podatke 48. člen ZDR-1, ki določa, da se lahko osebni podatki delavcev zbirajo, obdelujejo, uporabljajo in posredujejo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem. V praksi je praktično nemogoče, da delodajalec ne bi zbiral, obdeloval ali uporabljal osebnih podatkov svojih zaposlenih, saj npr. že samo vodenje evidence o zaposlenih predstavlja obdelavo oz. uporabo delavčevih osebnih podatkov (Bečan idr., 2016, str. 268). Tukaj gre predvsem za osebne podatke, ki omogočajo enolično identifikacijo posameznika, kot so ime in priimek, davčna številka, podatki o plači itd. Ob tem lahko osebne podatke delavcev zbira, obdeluje, uporablja in posreduje tretjim osebam samo delodajalec ali delavec, ki ga delodajalec za to posebej pooblasti. Prav tako se morajo osebni podatki delavcev, za zbiranje katerih več ne obstoji zakonska podlaga, takoj zbrisati in prenehati uporabljati. Če niso ti osebni podatki opredeljeni kot arhivsko gradivo, oziroma, če zakon ne določa drugače, se jih mora uničiti, izbrisati, blokirati ali anonimizirati. Podatki v zvezi z delovnim razmerjem, na primer podatki o kršitvah delovnih obveznosti, se lahko hranijo do konca delovnega razmerja ali do preteka zastaralnih rokov (Karlovšek idr., 2008, str. 51). V primerih, ko za obdelavo osebnih podatkov ni izrecno določene pravne podlage v zakonu, lahko delodajalec osebne podatke zaposlenih zbira, posreduje oz. obdeluje le s privolitvijo zaposlenega. Zaradi samega dokazila je priporočljivo, da je le-to podano v pisni obliki, vendar pa lahko zaposleni takšno soglasje brez kakršnihkoli posledic tudi odkloni. Če posameznik meni, da mu je bila iz strani delodajalca kršena pravica do varstva osebnih podatkov, je za uvedbo inšpekcijskega nadzora zoper delodajalca pristojen informacijski pooblaščenec. V primeru ugotovitve kršitve gre za kaznivo dejanje, posledico pa predstavlja odškodninska oz. civilna odgovornost za delodajalca (Bečan idr., 2016, str. 272).

Namen vzpostavitve ZVOP-1 je bil, da se sprejme takšna zakonodaja, ki posameznikom priznava osebne podatke kot del njihove zasebnosti, vendar obenem pooblaščenim osebam dopušča obdelavo le-teh, in sicer tam, kjer je to potrebno, oz. ko za to obstaja opravičljiv ali

z zakonom določen cilj, ter da se prepreči in kaznuje vse morebitne kršitve varstva osebnih podatkov (Pirc Musar, 2006). Z vzpostavitvijo ZVOP-1 je Republika Slovenija izpolnila svojo dolžnost do EU z implementacijo Direktive 95/46/ES, poleg tega prejšnji Zakon o varstvu osebnih podatkov (ZVOP, Uradni list RS, št. 59/99, 57/01, 59/01 – popr., 73/04 – ZUP-C in 86/04 – ZVOP-1), ni več sledil hitremu razvoju evropskega trenda varstva osebnih podatkov (Jacksteit, 2019). Že nekaj časa je v pripravi nov Zakon o varstvu osebnih podatkov (ZVOP-2), katerega predlog temelji na podlagi Splošne uredbe o varstvu osebnih podatkov (GDPR). Kljub temu da ZVOP-2 še ni sprejet, veljajo tudi v Sloveniji na področju varstva osebnih podatkov od 25. 5. 2018 določbe GDPR, saj se ta neposredno, brez izjeme uporablja v vseh državah članicah EU (Jamšek, 2018). Za tista področja, ki jih GDPR podrobneje ne ureja, do sprejetja novega ZVOP-2 veljajo še vedno določbe iz ZVOP-1 (Fakin, 2019).

V prvem členu ZVOP-1 so določene pravice, obveznosti, načela in ukrepi, s katerimi se preprečuje neustavne, nezakonite in neupravičene posege v zasebnost in dostojanstvo posameznika oz. posameznice pri obdelavi osebnih podatkov.

Osebni podatki se zbirajo zakonito in pošteno. Torej le pod pogoji, ki so določeni z zakonom in z načinom, ki je dopusten (2. člen ZVOP-1). Obdelava osebnih podatkov pomeni kakršnokoli avtomatizirano ali ročno dejanje, kot je npr. zbiranje, shranjevanje, posredovanje, spreminjanje, brisanje osebnih podatkov ipd. (6. člen ZVOP-1).

Po 6. členu ZVOP-1 se imenuje upravljalca z osebnimi podatki, ki pomeni vsako fizično, pravno ali drugo z zakonom določeno osebo, ki sama ali skupaj z drugimi določa sredstva in namen obdelave. Upravljalec z osebnimi podatki mora od posameznika, kjer ni zakonske podlage, pridobiti privolitev za obdelavo osebnih podatkov, ki je lahko podana pisno ali ustno. Po uredbi GDPR in predlogu ZVOP-2 je osebna privolitev posameznika še nekoliko strožje pogojena, saj je določeno, da mora upravljalec z osebnimi podatki za obdelavo osebnih podatkov (če za to ni zakonske podlage), od posameznika pridobiti privolitev, ki mora biti jasna, prostovoljna, brez prisile in negativnih posledic zaradi morebitne odklonitve. Tukaj gre za morebitne delovnopravne posledice, kjer posameznik nima možnosti odklonitve obdelave podatkov ali pa predstavlja pogoj za sklenitev posla posameznikova privolitev v obdelavo osebnih podatkov (Djinović, 2018).

Ocenjevanje dopustnega vpogleda v osebne podatke določa načelo sorazmernosti, katero natančneje opredeljuje 3. člen, in sicer, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo. Prav tako se osebni podatki lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače (16. člen ZVOP-1). 30. člen ZVOP-1 določa, da lahko posameznik od upravljalca z osebnimi podatki zahteva vpogled v osebne podatke, ki se obdelujejo, oz. nanašajo nanj.

Nekoliko drugače je varstvo osebnih podatkov določeno v javnem kot v zasebnem sektorju. Ta dva segmenta podrobneje urejata 9. in 10. člen ZVOP-1. Za javni sektor so določila strožja, saj določajo, da se lahko osebni podatki obdelujejo le na podlagi zakona. Če zakon tako določi, se lahko nekateri osebni podatki obdelujejo le s privolitvijo posameznika, zoper katerega se bodo obdelovali podatki, medtem ko se v zasebnem sektorju lahko osebni podatki obdelujejo, če njihovo obdelavo in konkretizacijo določa zakon ali če je posameznik v to osebno privolil (Pirc Musar, 2006). Po 37. členu uredbe GDPR in 46. členu predloga ZVOP-2 morajo organizacije, ki redno upravljajo z osebnimi podatki posameznikov, bodisi tudi z občutljivimi osebnimi podatki zaradi opravljanja storitev, obvezno imenovati pooblaščeno osebo za varstvo z osebnimi podatki, ki bo preverjala upoštevanje predpisov (Informacijski pooblaščenec, b. d.). Delovanje pooblaščene osebe mora biti neodvisno, brez pridobivanja navodil ter v sodelovanju s posamezniki, zoper katere se obdelujejo osebni podatki (Jamšek, 2018). Informacijski pooblaščenec ima kot državni nadzorni organ za varstvo osebnih podatkov po 37. členu ZVOP-1 pristojnosti izvrševanja inšpekcijskega nadzora nad upoštevanjem določb po ZVOP-1 ter drugih predpisov, ki urejajo varstvo osebnih podatkov, po 54. členu ZVOP-1 pa ima le-ta pristojnost tudi odrediti inšpekcijske ukrepe in opraviti preventivne inšpekcijske nadzore v organih javnega in zasebnega sektorja, odrediti anonimizacijo, izbris ali uničenje podatkov, če ugotovi, da so bili osebni podatki obdelani v nasprotju z zakonom.

ZEKom-1 ureja pogoje za zagotavljanje elektronskih komunikacijskih omrežij in izvajanje elektronskih komunikacijskih storitev, ureja zagotavljanje univerzalne storitve ter določa pravice uporabnikov. Med drugim ureja tudi varnost omrežij in varovanje pravice do komunikacijske zasebnosti uporabnikov javnih komunikacijskih storitev ter reševanje sporov na področju tega zakona (1. člen ZEKom-1).

8. točka 3. člena določa, da se za elektronsko pošto šteje vsako besedilno, slikovno, govorno, zvočno besedilo, poslano po javnem komunikacijskem omrežju, ki se lahko shrani v omrežju ali prejemnikovi terminalski opremi, dokler ga prejemnik ne prevzame. Uporabnik je fizična oseba, ki opravlja javno komunikacijsko storitev v zasebne ali poslovne namene, čeprav ni nujno, da je naročen nanjo (prvi odstavek 144. člena).

V 2. odstavku 145. člena, po katerem se zagotavlja varnost obdelave, je določeno, da morajo vsi vzpostavljeni ukrepi za zagotovitev varnosti, ob upoštevanju tehnološkega razvoja zagotoviti takšno raven varnosti in zavarovanja, ki bo ustrezala predvidenemu tveganju, ki ga predstavlja vsak poseg v tajnost, zaupnost in varnost elektronsko komunikacijskega omrežja.

147. člen podrobneje ureja zaupnost komunikacij. Njegov namen je varovanje pričakovane zasebnosti na področju uporabe elektronskih komunikacij ter zagotavljanje svobode izražanja in komuniciranja. Zaupnost komunikacij se nanaša na samo vsebino komunikacij,

prometne podatke in lokacijske podatke, dejstva in okoliščine v zvezi s prekinitvijo povezave, ali s tem, da povezava ni bila vzpostavljena.

Prometni podatki oz. podatki o prometu so katerikoli podatki, obdelani z namenom prenosa komunikacije po elektronskem komunikacijskem omrežju ali zaradi njegovega zaračunavanja (3. člen ZEK-om1). Tudi prometni podatki se štejejo za osebne podatke, ker se nanašajo na dejstvo, kdo s kom komunicira, kdaj, kako in zakaj. Med prometne podatke elektronske pošte se tako štejeta elektronska naslova pošiljatelja in prejemnika, datum in čas pošiljanja, vsebina sporočila ter različne priloge, npr. priponke (Zupančič, 2015). Ustavno sodišče RS je leta 2014 na pobudo informacijskega pooblaščenca razveljavilo obvezno hrambo prometnih podatkov po ZEKom-1, saj naj bi le-ti predstavljali nesorazmeren poseg v zasebnost posameznika (Pirc Musar, 2014).

5. odstavek 147. člena določa, da so vse oblike nadzora oziroma prestrezanja komunikacij, ki jih izvajajo tretje osebe in te niso uporabniki, udeleženi v komunikaciji, kot so poslušanje, prestrezanje, snemanje, shranjevanje in posredovanje komunikacij brez soglasja uporabnikov prepovedane, razen če je taka oblika nadzora oziroma prestrezanja nujno potrebna za prenos sporočil (npr. telefaks sporočila, elektronska pošta, elektronski predali, glasovna pošta, storitev SMS).

Snemanje in shranjevanje komunikacij brez predhodne privolitve udeležencev komunikacije je prepovedano tudi uporabnikom, kadar gre za komunikacije, kjer taka obdelava podatkov ni običajna in je udeleženci komunikacije zaradi njene narave ne pričakujejo in ne morejo vnaprej pričakovati (šesti odstavek 147. člena).

Evropska komisija je leta 2017 predstavila predlog nove uredbe o e-zasebnosti (ePrivacy Regulation), ki bi glede na razvoj elektronskih komunikacij enotno uredila področje digitalne zasebnosti za vse državljane EU, saj je zakonodaja v državah članicah na podlagi Direktive 2002/58/ES evropskega parlamenta in sveta z dne 12. 7. 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Uradni list EU, št. 201, z dne 31. 7. 2002) trenutno precej neenotna. Pri prvem predlogu je prišlo do zapletov, saj naj bi imele države članice po uredbi še večjo možnost nadzora nad državljani, prav tako s strani Komisije ni bilo podanih enotnih rešitev za hrambo prometnih podatkov (STA, 2020). Zaradi različnih mnenj in interpretacij pravil posameznih držav članic je bil februarja 2020 pripravljen nov predlog uredbe o e-zasebnosti, vendar se ta z vidika varstva pravic uporabnikov odmika od sedanje uredbe GDPR ter že obstoječega ZEKom-1. V predlogu je namreč premalo poudarka na varnosti meta podatkov in vsebine komunikacij, s katerimi lahko dejansko dobimo vpogled v življenje posameznika. Ponudniki elektronskih komunikacij bi morali imeti določena strožja pravila o sami obdelavi podatkov, s katerimi razpolagajo, prav tako bi morala nova uredba vsebovati jasna in strožja določila, kdaj lahko ponudniki elektronskih komunikacij dejansko obdelujejo podatke, jih delijo s tretjimi

osebami in v katerih primerih lahko do podatkov dostopajo organi pregona (Prelesnik, 2020).

3 ANALIZA PRIMERA BARBULESCU PROTI ROMUNIJI 61496/08

Primer Barbulescu proti Romuniji iz ESČP se dotika precej aktualnega in obenem problematičnega področja, kjer je na eni strani izražen interes posameznika, ki pričakuje določeno stopnjo zasebnosti, kljub temu da je na delovnem mestu, medtem ko si na drugi strani želi delodajalec z vpeljavo nadzora nad zaposlenimi preprečiti zlorabo uporabe službeno-elektronskih sredstev komunikacije v zasebne namene. V slednjem primeru je šlo za prikrit nadzor delodajalca nad elektronsko pošto zaposlenega oz. službenega klepetalnika, ki je sprva vodil v odpoved delovnega razmerja, nato v sodne postopke na nacionalni ravni, kasneje pa je spor med delavcem in delodajalcem prerasel v odmevno sodbo proti Romuniji, na podlagi katere je ESČP še bolj zaostril pogoje, pod katerimi so delodajalci upravičeni nadzorovati svoje zaposlene, z vidika preverjanja njihove internetne aktivnosti.

3.1 DEJANSKO STANJE

Romunski državljan Bogdan Mihai Barbulescu je na podlagi 34. člena EKČP vložil zahtevek za obravnavo na ESČP, zoper državo Romunijo. Države pogodbenice se s tem členom zavezujejo, da ne bodo na noben način ovirale izvajanje te pravice. Primer 61496/08 izvira z dne 15. 12. 2008.[1]

Tožnik je bil od 1. 8. 2004 do 6. 8. 2007 zaposlen v zasebnem romunskem podjetju, kot svetovalec v prodaji oz. prodajni inženir. Po navodilih delodajalca si je za potrebe komuniciranja s strankami ustvaril službeni Yahoo messenger račun, sicer je poleg tega že imel tudi zasebni račun. V internem pravilniku delodajalca je določeno, da bo vsaka motnja reda in discipline podjetja s strani zaposlenega kaznovana, slednja pa se navezuje tudi na zasebno uporabo računalnikov, telefonov in telefaksov. Interni pravilnik sicer ni striktno določal, da bo obstajala možnost nadzora komunikacije zaposlenih s strani delodajalca. Barbulescu se je s pravilnikom seznanil in ga tudi podpisal (20. 12. 2006), kar predstavlja dokazno gradivo, ki je bilo kasneje tudi posredovano sodišču prve stopnje v Romuniji. Leta 2007 so se morali vsi zaposleni v tem podjetju seznaniti z informativnim obvestilom, poslanim s strani vodstva, v katerem so bili seznanjeni z odpovedjo njihove sodelavke, po navedbah zaradi večkratnih disciplinskih prekrškov zoper nadrejenega ter neizpolnjevanja svojih delovnih nalog in med drugim tudi zasebne uporabe interneta, telefona in fotokopirnega stroja. V informativnem obvestilu je bilo zapisano tudi, da je delodajalec

[1] Besedilo te točke je povzeto po sodbi Evropskega sodišča za človekove pravice v primeru Barbulescu proti Romuniji v Strasbourgu, z dne 12. 1. 2016, pridobljeno s https://hudoc.echr.coe.int/fre-press#{"itemid":["001-159906"]}, ter z dne 5. 9. 2017, pridobljeno s https://hudoc.echr.coe.int/spa#{"itemid":["001-177082"]}

dolžan nadzorovati delovno aktivnost zaposlenih in vsako kršitev tudi kaznovati. Vsi zaposleni so morali podpisati kopijo sporočila, med njimi je bil tudi Barbulescu, ki je informativno sporočilo podpisal nekje v času med 3. 7. 2007 in 13. 7. 2007 (točen datum ni znan). Problem je nastal, ko je nekje v tem času delodajalec nadzoroval njegovo komunikacijo oz. preverjal njegovo internetno aktivnost in ga 13. 7. 2007 tudi pozval, naj mu pojasni zakaj je med službenim časom uporabljal internet oz. službeni Yahoo messenger za zasebne namene. Delodajalec je Barbulescuja seznanil z dejstvom, da je bila njegova internetna aktivnost nadzirana ter da o tem obstajajo dokazi. Kot dokaz mu je prikazal grafikone, ki so potrjevali, da je bila njegova internetna aktivnost večja od ostalih zaposlenih, vendar pa Barbulescu ni bil seznanjen s tem, da je bila nadzirana tudi sama vsebina njegovih sporočil. Ker je Barbulescu sprva zanikal zasebno uporabo službenega messengerja, ga je delodajalec ponovno pozval k priznanju, tokrat mu je kot dokaz priložil še 45 strani dolg izpisek, iz katerega je bila razvidna tudi vsebina sporočil, ki si jih je Barbulescu v tem času izmenjal z bratom in zaročenko, v zvezi z zasebnimi zadevami, nekatera so bila tudi intimne narave. Poleg teh sporočil je bil priložen še izpisek 5 sporočil, ki si jih je Barbulescu izmenjal z svojo zaročenko preko svojega osebnega messenger računa. Barbulescu je delodajalcu zatrdil, da mu je bila z njegovim dejanjem kršena pravica do tajnosti dopisovanja, kljub temu se je le-ta nekaj dni kasneje odločil, da Barbulescu na podlagi disciplinskega postopka prekine delovno razmerje. Barbulescu je kot tožnik odpoved pogodbe o zaposlitvi najprej izpodbijal na romunskem okrožnem sodišču, kjer je zahteval preklic odpovedi, izplačilo neplačanih zneskov v zvezi z zaposlitvijo, vrnitev na delovno mesto ter približno 30.000 € odškodnine. S svojimi zahtevami se je opiral na podobnosti primera Copland proti Združenemu kraljestvu, z argumentom, da so tako telefonski pogovori, kot komunikacije preko elektronske pošte zaposlenih zajete s pojmoma ''zasebno življenje'' in ''dopisovanje'', ki ju ščiti 8. člen EKČP. Barbulescu je trdil, da je bila njegova odpoved nezakonita ter da je delodajalec s spremljanjem njegovih komunikacij in dostopom do njene vsebine kršil tudi kazensko pravo (tč. 1, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23, 24, 25) (European Court of Human Rights, 2017).

Okrožno sodišče v Romuniji je v sodbi z dne 7. 12. 2007 zavrnilo tožnikov zahtevek in razsodilo, da je bila njegova odpoved zakonita. Odločitev sodišča je temeljila na dejstvih, da je delodajalec, preden je sprožil disciplinski postopek zoper zaposlenega, dvakrat pozval tožnika, da bi mu obrazložil svoja dejanja in mu dal možnost zagovora. Sodišče je prav tako zavzelo stališče, da delodajalčev nadzor komunikacij zaposlenega, ne glede na to, ali je upravičen ali ne, ni mogel izničiti veljavnosti disciplinskega postopka. Ker je Barbulescu zatrjeval, da je uporabljal službeni messenger samo v poslovne namene, iz delodajalčevega dokaza pa je razvidno nasprotno, je predstavljal izpisek vsebine komunikacije v tem primeru edini dokaz, iz katerega je razvidno, da je tožnik lagal. Sodišče je upoštevalo tudi dejstvo, da ima delodajalec legitimno pravico do nadzora zaposlenih, z vidika ugotavljanja namembnosti službene opreme (v tem primeru računalnika) ter preverjanja storilnosti

zaposlenih. Nadalje se je sodišče sklicevalo tudi na dejstvo, da so bili vsi zaposleni v podjetju predhodno seznanjeni z odpovedjo njihove sodelavke, med drugim prav tako zaradi rabe službene opreme v zasebne namene in da je dal delodajalec na ta način zaposlenim jasno opozorilo o možnosti nadzora. Sodišče je prav tako menilo, da so takšni pregledi s strani delodajalca potrebni za primere različnih tveganj, ko bi lahko zaposleni poškodovali informacijsko tehnologijo podjetja, bodisi razkrili poslovne skrivnosti, ki bi lahko podjetju prinesle škodo. Okrožno sodišče v Romuniji je tako razsodilo, da je tožnik storil disciplinski prekršek prepovedi uporabe službenega računalnika v zasebne namene, za katero je predpisan disciplinski postopek, sankcija pa je predstavljala odpoved pogodbe o zaposlitvi. S tem je sodišče Barbulescujevo pritožbo zavrglo kot neutemeljeno (tč. 28) (European Court of Human Rights, 2017).

Barbulescu se je nato pritožil na pritožbeno oz. prizivno sodišče v Bukarešti, kjer je poleg navedenih argumentov pred sodiščem 1. stopnje navajal še, da predhodno sodišče ni pretehtalo posameznih interesov v primeru in je nepravično presodilo prednost interesu delodajalca. Poleg tega je zatrjeval, da tako interni predpisi delodajalca, kot informativno obvestilo niso jasno predvidevali možnosti delodajalčevega nadzora nad komunikacijo zaposlenih. Sodišče je v sodbi z dne 17. junija 2008 Barbulescujevo pritožbo zavrnilo z argumenti, da je prvostopenjsko sodišče ravnalo pravilno, z vidika ugotovitve, da je internet orodje, ki ga daje delodajalec na voljo zaposlenim za opravljanje nalog, ki spadajo v opis dela in lahko s tem namenom postavi tudi svoja pravila uporabe le-tega. Sodišče se je oprlo tudi na dejstvo, da so bili zaposleni o uporabi službene opreme obveščeni v internem pravilniku. Ker je šlo v slednjem primeru za konflikt med delodajalčevo pravico do nadzora in delavčevo pravico do zasebnosti, je sodišče svojo razsodbo utemeljilo na podlagi direktive 95/46/ES, ki določa smernice v zvezi z nadzorom nad uporabo e-pošte in interneta na delovnem mestu. Prvo je načelo nujnosti, po katerem je nadzor nujno potreben za dosego določenega cilja. Sledi mu načelo specifikacije namena, po katerem se morajo podatki zbirati le za točno določene, izrecne in zakonite namene. Po načelu preglednosti mora delodajalec zaposlene vedno obvestiti o možnosti nadzora in pred samo uvedbo le-tega, načelo legitimnosti pa določa, da se lahko procesi v zvezi z obdelavo osebnih podatkov zbirajo le z namenom, določenim na podlagi zakona. Sledita še načelo sorazmernosti, po katerem morajo biti izvedeni ukrepi v zvezi z nadzorom osebnih podatkov sorazmerni glede na namen, torej ne pretirani, ter načelo varnosti, kjer mora delodajalec sprejeti vse varnostne ukrepe, s katerimi zagotovi, da zbrani podatki niso na voljo tretjim osebam. Pritožbeno sodišče je razsodilo, da ima delodajalec pravico zagotoviti nemoten potek dela in je v ta namen upravičen nadzirati, kako zaposleni opravljajo svoje naloge, saj mu to določajo disciplinska pooblastila. Ker je tožnik zanikal navedene obtožbe, sodišče pritrjuje, da ni bilo mogoče doseči cilja na drugačen način kot s tem, da je delodajalec kršil tajnost pravice do dopisovanja zaposlenega. Sodišče je odločilo, da je bila sodba okrožnega sodišča zakonita in utemeljena, pritožba je bila zavrnjena (tč. 29, 30) (European Court of Human

Rights, 2017).

3.2 ODLOČITEV MALEGA SENATA

Po tem, ko Barbulescu na nacionalnih sodiščih ni dosegel uspeha, se je pritožil še na ESČP. Mali senat je 12. 1. 2016 razsodil, da je pritožba Barbulescuja, vložena na podlagi 8. člena EKČP, v konkretnem primeru ustrezna, saj se zadeva nanaša na varovanje človekovih pravic, z vidika spoštovanja človekovega zasebnega življenja, doma, družine in korespondence, torej je predmet spora dejansko objekt varovanja 8. člena EKČP. Se pa po mnenju malega senata slednji primer glede na koncept razumnega pričakovanja zasebnosti razlikuje od primerov Halford proti Združenemu kraljestvu ter Copland proti Združenemu kraljestvu, na podlagi katerih je sodišče odločalo v preteklosti (pri obeh je bila priznana kršitev 8. člena EKČP), z argumentom, da so bila v internem pravilniku podjetja, v katerem je bil Barbulescu zaposlen, določena pravila, ki so prepovedovala uporabo službene opreme za zasebne namene (tč. 56) (European Court of Human Rights, 2017). Romunska vlada je v svoji obrambi med argumenti navedla, da je tožnik zanikal uporabo službenega Yahoo messengerja v zasebne namene, zato ne more zahtevati pravice do zasebnosti, če jo obenem zanika. Tožnik med drugim ni pojasnil, zakaj je uporabljal službeno opremo za zasebne namene. Kot razlog je navedel le, da je imel v službenem času malo strank ter da so bili stroški mobilne opreme v tistem času visoki. Sodišče je pritrdilo, da se je s fotokopijo sporočil dejansko posegalo v tožnikovo zasebnost, obenem pa je upoštevalo tudi dejstvo, da v postopkih pred nacionalnimi sodišči vsebina sporočil ni bila odločilnega pomena, saj je bila fotokopija namenjena le dokaznemu gradivu, da so se tožnikova sporočila nanašala na njegovo zasebno, ne poslovno življenje. Tožnik se je pred malim senatom pritožil tudi glede 6. člena EKČP, ki določa, da ima vsakdo pravico do poštenega sojenja. Menil je, da sodišča niso opravila svoje dolžnosti pri varovanju njegovih interesov, prav tako je trdil, da ni imel možnosti predstaviti svojih prič. Ker je tožnikov delodajalec prekinil delovno razmerje zaradi kršitve uporabe službene opreme v zasebne namene, je sodišče ugotavljalo, če so pristojna sodišča v Romuniji ustrezno pretehtala interese delodajalca in interese zaposlenega. Mali senat je ugotovil, da je imel tožnik možnost izjaviti se pred pristojnimi sodišči v Romuniji in zahtevati pravico v zadostni meri, brez vpoklica svojih prič, prav tako naj bi imel delodajalec vpogled v vsebino zasebnih sporočil zaposlenega šele po tem, ko je tožnik že storil disciplinski prekršek oz. se je delodajalcu že zlagal o neuporabi službene opreme v zasebne namene. Prav tako je bil nadzor delodajalca omejen zgolj na rabo Yahoo messengerja. Ker so v preteklih primerih že nastajale materialne škode, povzročene delodajalcu s strani zaposlenega, sodišče tako priznava legitimen interes delodajalca do nadzora nad službeno-komunikacijsko opremo zaposlenega in na podlagi predstavljenih dejstev ugotavlja, da so nacionalna sodišča ustrezno zastopala interes posameznika. Mali senat je s 6 glasovi proti 1 tako razsodil, da ni prišlo do kršitve 8. člena EKČP (tč. 24, 30, 56, 57, 58, 59, 63, 64, 65) (European Court of Human Rights, 2016).

3.3 DELNO ODKLONILNO MNENJE SODNIKA ALBUQUERQUEJA

Paulo Pinto De Albuquerque je portugalski sodnik ESČP od leta 2011. Pred tem je bil med drugim sodnik lizbonskih sodišč, svetovalec portugalskega ministrstva za notranje zadeve, profesor prava na Univerzi v Illinoisu, od leta 2015 pa je profesor prava na Pravni fakulteti Katoliške Univerze v Lizboni (Sistema penale, 2019). Sodnik je v prvi točki odklonilnega mnenja pojasnil, da predstavlja primer Barbulescu proti Romuniji nadzor nad rabo interneta na delovnem mestu, ter da se strinja z ugotovitvijo večine, da predstavlja predmet spora 8. člen EKČP. Ne strinja pa se z razsodbo malega senata, v kateri je bilo določeno, da je bil delodajalčev nadzor v konkretnem primeru upravičen. V drugi točki pojasnjuje, da je slednji primer predstavljal odlično priložnost za ESČP, da bi lahko razvilo sodno prakso glede varovanja človekovih pravic z vidika nadzora nad rabo interneta na delovnem mestu, saj se je v slednjem primeru dejansko stanje nanašalo na še neobstoječo politiko nadzora interneta, vprašanje pravilno izvedenega nadzora delodajalca ter osebne in občutljive podatke zaposlenega, ki so bili delodajalcu vidni in razkriti v teku disciplinskega postopka. Sodnik je med drugim izpostavil, da je dostop do interneta človekova pravica, s katero lahko posameznik izraža svoje mnenje, prav tako posamezniku predstavlja vir informacij. Izpostavil je tudi pomanjkljivost, oziroma odsotnost delovnopravne zakonodaje glede rabe interneta na delovnem mestu, saj je v konkretnem primeru v delovnem okolju obstajal le interni pravilnik podjetja, ki je prepovedoval zasebno rabo. Opozoril je tudi na pomanjkanje zanesljivega dokaza, da so bili zaposleni v slednjem podjetju dejansko seznanjeni z možnostjo nadzora njihove komunikacije na način, da je bil na njihov računalnik naložen program, ki je delodajalcu poleg nadzora njihovih komunikacij omogočal še pripravo statistike dnevne rabe interneta zaposlenih. V 19. točki odklonilnega mnenja sodnik poudarja občutljivost osebnih podatkov, ki so bili predmet korespondence, saj je bil predmet dopisovanja tudi zdravstvene in spolne narave, poleg tega je imel delodajalec vpogled tudi v osebni messenger račun, ki ni bil v nikakršni povezavi z delovnim mestom. Sodnik meni, da je bila prekinitev delovnega razmerja v konkretnem primeru pretirana, saj tožnik s svojim početjem delodajalcu dejansko ni povzročil nobene dokazljive škode. V zaključku navaja, da zaposleni, kljub temu da so na delovnem mestu, ne morejo popolnoma opustiti svojega zasebnega življenja, nove tehnologije pa lahko delodajalcu še bolj olajšajo dostop do zasebnosti zaposlenih, ne da bi se le-ti tega zavedali. Sodnik meni, da pristojna sodišča niso pravilno postopala pri ugotavljanju razumnosti delodajalčeve odpovedi, storjene zaradi disciplinskega prekrška in delavcu iz tega vidika niso zagotovila zadostnega pravnega varstva (tč. 1, 2, 3, 16, 17, 19, 21, 22, 23) (European Court of Human Rights, 2016). Uvedba novih tehnologij omogoča nove možnosti nadzora nad zaposlenimi, zato zahteva tudi razvoj nove sodne prakse na tem področju. Mali senat bi moral ne zgolj presojati, če so romunska sodišča pravilno postopala pri varovanju tožnikove pravice, temveč tudi dejansko tehtati tako med interesom delavca kot delodajalca, saj bi potem lahko odločal drugače in dejansko vzpostavil novo sodno prakso na tem področju.

3.4 ODLOČITEV VELIKEGA SENATA

Po zavrnjeni pritožbi malega senata se je Barbulescu pritožil še na Veliki senat. Sodišče je o pritožbi odločalo 5. 9. 2017. Romunska vlada se je v obrambi oprla na dodatne argumente v utemeljitvi, da 8. člen EKČP v slednjem primeru ni bil uporabljen. Ni namreč obstajal dokaz, da je bila fotokopija tožnikovih komunikacij dejansko razkrita njegovih sodelavcem, prav tako je tožnik predložil fotokopijo sporočil v postopku pred domačimi sodišči sam. Nacionalni organi so tako fotokopijo prepisa sporočil uporabili zgolj kot dokazno gradivo, kar je tožena stranka tudi sama zahtevala. Tožnik je svoje argumente ponovno predstavil še pred Velikim senatom. Zatrjeval je, da je kot edina oseba z geslom svojega službenega messenger računa utemeljeno pričakoval komunikacijsko zasebnost. Prav tako ga delodajalec ni predhodno obvestil o možnosti nadzora njegovih komunikacij. Sodišče meni, da lahko pojem zasebnega življenja vključuje tudi poklicne dejavnosti, saj ima večina ljudi tudi med delovnim časom priložnost za razvijanje odnosov in s tem ugotavlja, da je t. i. sporna internetna storitev obliki messengerja le ena izmed neposrednih storitev komunikacije, ki posameznikom omogoča zasebno življenje. Tako pošiljanje kot prejemanje sporočil zajema pojem ''dopisovanje'', četudi so poslane iz računalnika delodajalca, kljub temu da je delodajalec zaposlenim naročil, da se vzdržijo osebnih dejavnosti na delovnem mestu. Sodišče nadalje ugotavlja, da je delodajalec vzpostavil sistem za spremljanje uporabe interneta svojih zaposlenih, z namenom, da bi preverjal njihovo upoštevanje internih predpisov, in obenem pritrjuje, da je bil tožnik obveščen o prepovedi uporabe službenega interneta v zasebne namene, ni pa bilo jasno, ali je bil tožnik obveščen tudi pred samo uvedbo nadzora. Kljub temu da je tožnik podpisal informativno sporočilo o odpovedi njegove sodelavke nekje med 3. in 13. julijem 2007, domača sodišča niso preverila, ali je bil tožnik o tem dejansko obveščen pred datumom začetka nadzora, glede na to, da je delodajalec nadzoroval njegovo komunikacijo nekje med 5. in 13. julijem 2007. Iz navedenih dejstev namreč ni moč videti, da bi bil tožnik vnaprej obveščen o samem vpogledu in obsegu vpogleda v vsebino nadzora njegove komunikacije. Sodišče se sprašuje, v kolikšni meri omejevalni predpisi delodajalca tožniku dopuščajo razumno pričakovanje zasebnosti, saj interna navodila delodajalca ne morejo zmanjšati delavčevega družbenega življenja, četudi je na delovnem mestu povsem na nič. Tožnik je nadalje navedel argument, da je treba razlikovati med osebno uporabo interneta z namenom dobička ter majhnim ''neškodljivim'' zasebnim pogovorom, s katerim ni imel namena delodajalcu povzročiti nikakršne škode niti pridobiti nobenega dobička. Izpostavil je tudi razvoj IKT in družbene navade, povezane z njeno uporabo. Navaja, da nacionalna sodišča niso izpolnila svojih pravnih obveznosti, saj njegove odpovedi niso razveljavila, čeprav so priznala, da je prišlo do kršitve zasebnosti njegovih komunikacij. Poleg tega trdi, da ga je delodajalec nadziral in mu šele nato dal možnost razjasnitve, ali so njegove komunikacije zasebne ali povezane z delom. Kršitev pritožnikove pravice do spoštovanja zasebnega življenja in dopisovanja je bila tako namerna in nezakonita, njen cilj pa je bil pridobivanje dokaznega gradiva, ki je omogočil odpoved

pogodbe o zaposlitvi. Tožnik na tej točki poziva sodišče, naj prizna kršitev 8. člena EKČP in s tem izkoristi priložnost za potrditev, da se spremljanje dopisovanja zaposlenih lahko izvaja le v skladu z veljavno zakonodajo, transparentno ter da delodajalec v slednjem primeru ni užival diskrecijske pravice nad nadzorom. Vlada v argumentih navaja, da so pristopi med državami članicami Sveta Evrope pri urejanju nadzora delodajalcev različni. Nekatere članice so to področje vključile v širši obseg obdelave osebnih podatkov, druge pa so na tem področju sprejele posebno zakonodajo. Tudi med njimi ni enotnih rešitev glede namena in obsega spremljanja s strani delodajalca, morebitnega predhodnega obveščanja ali osebne uporabe interneta med službenim časom. Naloga sodišča v tej zadevi je razjasniti naravo in obseg pozitivnih obveznosti države članice pri zaščiti pritožnikove pravice do spoštovanja zasebnega življenja in dopisovanja v okviru njegove zaposlitve, pri čemer sodišče priznava, da potrebnih ukrepov ni mogoče najti le v delovnem pravu, temveč tudi v civilnem in kazenskem pravu. V zvezi s tem sodišče delovnemu pravu priznava posebne značilnosti, kjer gre za pogodbeno razmerje med delodajalcem in delojemalcem, določeno s pravicami in obveznostmi na obeh straneh, zanj pa je značilna enostranska podrejenost. Delovno pravo dopušča prostor za pogajanja v pogodbi o zaposlitvi, sicer pa morajo stranke tudi same urediti del sodelovanja. Glede na to sodišče meni, da se mora državam pogodbenicam pri vzpostavitvi pravnega okvirja, ki ureja pogoje, pod katerimi lahko delodajalec nadzoruje elektronsko komunikacijo neprofesionalne narave, zagotoviti široko polje proste presoje, kljub temu pa diskrecija ne more biti neomejena. Sodišče se zaveda hitrega dogajanja na tem področju, zato na tej točki postavlja merila, katera bodo morali nacionalni organi pri nadaljnji presoji tudi upoštevati. Nacionalni organi morajo pravilno ugotoviti, ali je bil delavec s strani delodajalca vnaprej obveščen o možnosti spremljanja, oziroma nadzora njegove korespondence, pri čemer morajo upoštevati, da mora biti obvestilo izvedeno na primeren način (obvezno pred začetkom nadzora, najboljše je v pisni obliki, da obstaja zanesljiv dokaz). Sodišča morajo pri svoji presoji upoštevati tudi, ali so bile spremljane vse komunikacije zaposlenega ali le del njih (ali se spremljajo le prometni podatki ali tudi vsebina sporočil), ali je bil nadzor časovno omejen, in število ljudi, ki je imelo dostop do rezultatov. Sodišča morajo nadalje upoštevati, ali je delodajalec utemeljil spremljanje komunikacij in dostop do njihove dejanske vsebine ter ali bi bilo mogoče vzpostaviti manj vsiljiv način spremljanja, kot je z neposrednim dostopom do vsebine komunikacij zaposlenega oz. nadzor z manj vsiljivimi metodami in ukrepi, kot z neposrednim dostopom do vsebine komunikacij. Za vsak primer posamezno je treba opredeliti, ali bi bilo delodajalčev cilj možno doseči, ne da bi imel neposreden dostop do vsebine komunikacij, pretehtati, kakšne so posledice nadzora za zaposlenega, v kakšen namen bo delodajalec uporabil rezultate nadzora ter ali je bil zaposlenemu zagotovljen ustrezen zaščitni ukrep pri varovanju svoje pravice do zasebnosti. Sodišče odloči, da navedbe tožnika v zvezi z domnevnim razkritjem vsebine sporočil s strani delodajalca ostalim zaposlenim niso dovolj podkrepljene, saj tožnik ni predložil nobenega nadaljnjega dokazila, ki bi to povsem

potrjevala. Sodišče je ugotovilo tudi, da nacionalna sodišča niso dovolj preučila vprašanja stopnje vdora v zasebnost tožnika, prav tako niso opravila ustrezne presoje, ali obstajajo utemeljeni razlogi, ki bi opravičevali spremljanje sporočil. Ni bilo namreč navedenega jasnega razloga, zakaj se je delodajalec odločil ravno v tistem času nadzorovati aktivnosti zaposlenih. Tako okrožno kot pritožbeno sodišče v Romuniji nista dovolj preučili, ali bi bilo mogoče cilj delodajalca doseči z manj invazivnimi metodami, ter preučili nujnost najstrožjega disciplinskega postopka, katerega posledica je bila prekinitev delovnega razmerja. Nazadnje sodišče ugotavlja, da domača sodišča niso ugotovila, kdaj je delodajalec do vsebine sporočil dejansko dostopal. Na tej točki se opre na priporočilo odbora ministrov Sveta Evrope CM/Rec (2015) 5, ki narekuje, da mora biti delavec v skladu z načelom transparentnosti vselej obveščen o zbiranju podatkov, ki se nanašajo nanj. Prav tako nacionalna sodišča niso ugotovila, ali je delodajalec o možnosti nadzora predhodno obvestil zaposlenega. Niso niti presodila razlogov, ki bi opravičevali ukrepe delodajalca, ter če bi bil lahko v slednjem primeru uporabljen milejši ukrep za dosego cilja, kot je nadzor nad vsebino sporočil in nenazadnje prekinitev samega delovnega razmerja. Sodišča bi morala presoditi, ali je do vsebine sporočil dovoljeno dostopati brez vednosti osebe, na katero se nanašajo. Veliki senat je z argumentom, da nacionalni organi in mali senat niso zagotovili ustrezne zaščite pritožnikove pravice do spoštovanja zasebnega življenja, doma in korespondence z 11 glasovi proti 6 razsodilo kršitev 8. člena EKČP. Sodniki bistvene odškodnine Barbulescuju niso prisodili, saj so bili mnenja, da že sama ugotovitev kršitve pravice do zasebnosti oz. zmaga pred Velikim senatom tožniku predstavlja pravično zadoščenje. Toženi državi so naložili zgolj poplačilo stroškov sodbe tožniku. Ayşe Işıl Karakas, turška sodnica ESČP od leta 2008, med drugim profesorica mednarodnega prava in prodekanja na Univerzi v Galatasarayu (PeoplePill, b. d.), v svojem ločenem odklonilnem mnenju pove, da se v celoti strinja z ugotovitvijo kršitve 8. člena EKČP, ne strinja pa se z mnenjem večine, da predstavlja že sama ugotovitev kršitve pravično zadoščenje za nepremoženjsko škodo, ki jo je tožnik utrpel. Sodišče lahko v skladu z 41. členom določi nek znesek, mišljen kot ''nagrado'' v zvezi z nepremoženjsko škodo, če meni, da je to potrebno, vendar lahko sodišče v takšnih primerih meni, da že sama ugotovitev kršitve pomeni pravično zadovoljstvo. V slednjem primeru nacionalna sodišča niso zagotovila ustrezne zaščite tožnikove pravice do spoštovanja zasebnega življenja in dopisovanja, zato je bil tožnik zaradi odpovedi delovnega razmerja resno oškodovan. Sodnica meni, da je v slednjem primeru ugotovitev kršitve 8. člena EKČP nedvomno tožniku povzročila nepremoženjsko škodo, zato si je sama prizadevala za podelitev skromnega zneska kot pravično zadovoljstvo tožene stranke (tč. 54, 66, 68, 71, 74, 75, 77, 78, 80, 84, 85, 86, 89, 92, 98, 114, 116, 117, 118, 119, 121,126, 136, 137, 138, 140, 141) (European Court of Human Rights, 2017).

3.5 SKUPNA ODKLONILNA MNENJA SODNIKOV

Sodniki Velikega senata se strinjajo z dejstvom, da je bilo treba pritožbo obravnavati s

stališča pozitivnih obveznosti države ter s splošnimi načeli oz. kriteriji, ki so bili postavljeni v prihodnjo presojo nacionalnim organom na tem področju. Kljub temu se ne strinjajo z večino, da domači organi niso zagotovili ustrezne zaščite tožnikove pravice do spoštovanja zasebnega življenja in dopisovanja, ter argumentom, da nacionalna sodišča posledično niso uspela vzpostaviti pravičnega razmerja med nasprotujočimi si interesi. Navajajo, da so dejstva v tej zadevi precej manj resna od drugih podobnih primerov, saj se je navsezadnje sodišče ukvarjalo z očitki o kršitvi človekove psihološke integritete s strani druge osebe. Prav tako ni točno določenega evropskega soglasja glede sprejetih ukrepov nacionalnih sodišč, saj je takrat le 6 od 24 anketiranih držav članic Sveta Evrope zakonsko uredilo področje zasebnosti na delovnem mestu. Sodniki navajajo, da je tožnik sprva pred nacionalnimi sodišči le izpodbijal odpoved delovnega razmerja, šele kasneje je na podlagi sodne prakse ESČP glede na primer Copland proti Združenemu kraljestvu trdil, da je njegova odpoved nezakonita in da delodajalec z dostopom in spremljanjem vsebine njegovih komunikacij krši pravo. Če ne obstaja zadosten dokaz, da tožniku domača pravna sredstva niso bila na voljo ali bila dovolj učinkovita, menijo, da ni podlage, na kateri bi sodišče lahko ugotovilo kršitev 8. člena EKČP. Kljub temu da je bila večina sodnikov Velikega senata osredotočena zgolj na analizo nacionalnih delovnih sodišč, sodniki v skupnem odklonilnem mnenju menijo, da leta ni bila pomanjkljiva do te mere, da bi lahko pripeljala do ugotovitve kršitve 8. člena. Romunski sodišči sta upoštevali interna pravila delodajalca ter dejstvo, da se je tožnik seznanil z njimi. Sodniki ne vidijo podlage za odstopanje njunih odločitev in menijo, da bi tožnik lahko pričakoval, da bo njegova aktivnost komunikacij nadzirana. Ugotavljajo, da sta sodišči ustrezno izvedli tehtanje med interesi, pri čemer sta upoštevali tako tožnikovo pravico do zasebnosti kot interese delodajalca, vključno s pravico do nadzora in ustreznimi disciplinskimi pooblastili za zagotovitev nemotenega poslovanja podjetja. Po mnenju sodnikov odločitev nacionalnih organov, da dodeli prednost delodajalčevemu interesu pred pritožnikovem, sama po sebi ne more sprožiti vprašanja v skladu z EKČP, saj so romunska sodišča ravnala v skladu z svojo zakonodajo. Prav tako tožnik ni nikoli trdil, da je njegov delodajalec nadzoroval karkoli izven okvira poklica oz. službe. Večina sodnikov, ki je podalo skupno odklonilno mnenje, se na tej točki strinja, da vlagatelj ni utemeljil svojih navedb, da je bila vsebina korespondence dejansko razkrita tudi njegovim kolegom. Nadalje argumentirajo, da so nacionalna sodišča pri svoji odločitvi v veliki meri upoštevala disciplinski postopek, v katerem je tožnik zanikal uporabo sredstev delodajalca za zasebne namene, kar je bilo napačno. Tožnik prav tako ni zanikal, da je bil seznanjen z informativnim sporočilom, vendar se ni mogel spomniti, kdaj ga je prejel. Nazadnje sodniki navajajo, da morajo delovna razmerja temeljiti na medsebojnem zaupanju, zato bi lahko tudi na podlagi tega nacionalna sodišča dosodila, da je zaposleni kršil zaupanje delodajalca. Zato menijo, da so nacionalna sodišča ustrezno izpolnila svojo dolžnost, da bi zaščitila delodajalca in s tem do kršitve 8. člena EKČP po njihovem mnenju v slednjem primeru ni prišlo (tč. 1, 2, 4, 5, 10, 11, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27) (European Court of Human Rights, 2017).

Odločitev Velikega senata je bila v tem primeru drugačna od razsodbe malega senata. Da bi lahko razumeli, zakaj je temu tako, narekuje dejstvo, da je pravzaprav naloga Velikega senata, katerega sestavlja 17 sodnikov namesto 7, odločiti se na novo, neodvisno od prejšnjih ugotovitev, kjer se praviloma lahko zgodi, da bo odločitev drugačna. V slednjem primeru dopustnosti delodajalčevega nadzora nad elektronskimi sredstvi komunikacije zaposlenega sodišče ni ugotavljajo prvič, saj je v preteklosti podobno odločalo že v primeru Copland proti Združenemu Kraljestvu ter drugimi. Primer je poseben iz tega vidika, ker je sodišče prvič odločalo o nadzoru delodajalca, ki prihaja iz zasebnega sektorja, saj je bilo podjetje, v katerem je bil Barbulescu zaposlen, zasebno. Iz sodbe kljub temu ne izhaja, da delodajalci pod nobenim pogojem ne smejo pregledati elektronske pošte zaposlenega ali da ga ne smejo odpustiti zaradi zasebne rabe interneta. Sodišče podaja smernice, ki jih morajo države članice ob podobnih primerih upoštevati, predvsem, da bi se izognile tožbam na ESČP v prihodnosti – več o tem v točki 4 (Unit, 2017).

4 POMEN PRIMERA BARBULESCU ZA RS

Že odločitev malega senata iz leta 2016 je vzbudila zanimanje tako širše kot tudi slovenske javnosti, saj je na spletu možno zaslediti veliko člankov v zvezi z slednjim primerom. V zvezi z razsodbo prvostopenjskega sodišča so si mnogi takrat sodbo razlagali kot, da imajo delodajalci dovoljenje do popolnega nadzora nad svojimi zaposlenimi (Mušič, b. d.). Ne glede na to, sodba na prvi stopnji za Slovenijo iz zakonodajnega vidika ni imela bistvenega pomena, saj ESČP dopušča državam članicam prosto presojo pri ureditvi pravil na področju delodajalčevega nadzora nad službeno-komunikacijsko opremo zaposlenega, z upoštevanjem mednarodnih pravnih virov. Pri nas je komunikacijska zasebnost še strožje varovana, saj je poseg v to pravico dopusten celo le z odredbo sodišča (Mušič, b. d.). Sicer je bila želja po zakonski ureditvi zasebnosti na delovnem mestu v Sloveniji prisotna že leta 2009, ko je to stališče zagovarjala tedanja informacijska pooblaščenka, prav tako so leta 2014 podali predlog zakona o zasebnosti na delovnem mestu državljani sami, pa vendar zakonodajna oblast potrebe po tem ni zaznala (Zupančič, 2015). Dejstvo je, da v slovenski zakonodaji še vedno ni točno določenih pravil glede delodajalčevega nadzora nad informacijsko-komunikacijskimi sredstvi delavca, kot veljajo posebna določila npr. za videonadzor na delovnem mestu (Bečan idr., 2016, str. 261), zato se na tem področju pravila izoblikujejo na podlagi že obstoječe evropske zakonodaje in ustaljene sodne prakse.

Odločitev Velikega senata postavlja delodajalcem strožja pravila, saj sama prepoved uporabe službeno-komunikacijske opreme zaposlenega v zasebne namene v internem aktu delodajalca, le-temu ne predstavlja zadostne oz. zakonite podlage za njegov nadzor nad vsebino sporočil, zato lahko ta s tem nezakonito poseže v delavčevo pravico do komunikacijske zasebnosti (Jadek & Pensa, 2017). 8 člen Ustave RS določa, da morajo biti zakoni v skladu s splošno veljavnimi načeli mednarodnega prava in z mednarodnimi pogodbami, ki obvezujejo Slovenijo, torej bi bila na tej podlagi sodba ESČP pravno zavezujoča za Slovenijo, če bi v njej posameznik, neprofitna organizacija itd. tožili Slovenijo. Vendar pa so nacionalna sodišča v skladu z 8. členom URS vezana tudi na EKČP. Tako odmevne sodbe, v katerih razsoja ESČP, pustijo nova pravna dejstva, razvije se nov sodni precedens, ki ga pri nadaljnji sodni praksi upoštevajo, bodisi se nanj oprejo tudi nacionalna sodišča v celotnem evropskem prostoru. Nacionalna sodišča oz. sodniki morajo za neposredno uporabo EKČP pri razsojanju v praksi tudi dobro poznati sodno prakso ESČP (Žgur, Šalamon & Koritnik, 2017). Leta 2018 se je v sodbi Višjega delovnega in socialnega sodišča, sklep pdp. 492/2018, sodišče v svoji odločitvi med drugim že oprlo oz. argumentiralo svojo odločitev tudi na podlagi primera Barbulescu proti Romuniji. Kljub temu da je šlo v slednjem primeru za vpogled v datoteke, ki so se nahajale na trdem disku službenega računalnika, ne v službeno elektronsko pošto, je sodišče ugotovilo, da gre za podobno problematiko – varovanje zasebnih podatkov na službenem računalniku. Višje

delovno sodišče je v slednjem primeru odločilo, da je delodajalec nezakonito vpogledal v službeni računalnik zaposlenega, saj bi ta moral zaposlenega o morebitni možnosti nadzora predhodno obvestiti. Sodišče se je prav tako oprlo na določbo iz primera Barbulescu proti Romuniji, kjer je ESČP razsodil, da mora imeti zaposleni vedno na voljo ustrezno pravno varstvo ob zlorabi takšnega nadzora. Pred tem je bilo sicer v slovenski sodni praksi primerov, ki bi se nanašali na koncept pričakovane zasebnosti na delovnem mestu, malo. Kot primer delodajalčevega dopustnega vpogleda v službeno elektronsko pošto zaposlenega določuje sodba Višjega delovnega in socialnega sodišča, sklep pdp. 69/2015, kjer je bilo razsojeno, da je delodajalec upravičen pregledati komunikacijo, ki jo je imel delavec v okviru opravljanja delovnih nalog. Elektronska pošta, ustvarjena za potrebe komuniciranja s strankami v imenu delodajalca, tako ne predstavlja varstva zasebnosti (Prelesnik, 2017).

V 121. točki sodbe je ESČP določilo kriterije, ki jih bodo morala nacionalna sodišča v podobnih primerih pri tehtanju med interesom delodajalca in delavca oz. pri opravljanju testa sorazmernosti tudi upoštevati. V kolikor nacionalna sodišča ne bodo postopala po slednjih smernicah, jih v podobnih primerih, če bo prišlo do same tožbe, na ESČP lahko čaka negativen izid, saj bo tudi nadaljnja sodna praksa ESČP v podobnih primerih naklonjena delavcem:

1. Ali je bil delavec vnaprej obveščen s strani delodajalca o možnosti nadzora oz. spremljanja njegove korespondence?
2. Ali so bile spremljane vse komunikacije ali le del njih (ali se spremljajo le prometni podatki ali tudi vsebina sporočil)? Ali je bil nadzor časovno omejen? Število ljudi, ki je imelo dostop do rezultatov (omejen dostop do podatkov)?
3. Ali je delodajalec utemeljil razlog za spremljanje komunikacij in dostop do njihove dejanske vsebine (ker je spremljanje vsebine komunikacij precej invazivna metoda, zahteva tehtnejšo utemeljitev)?
4. Ali bi bilo za dosego cilja možno uporabiti manj invaziven ukrep spremljanja, kot je vpogled v vsebino komunikacij?
5. Je potrebno tehtanje med posledicami nadzora za delavca ter ali so lahko rezultati nadzora sploh uporabljeni za dosego cilja nadzora?
6. Ali je imel delavec na voljo zadostna varovala (zlasti, ko gre za precej vsiljivo metodo nadzora)?

Ko govorimo o elektronski pošti, moramo vedeti, da uredba GDPR ščiti le prometne podatke, samo kršitev tajnosti vsebine zasebnih sporočil pa sankcionirata določila po Kazenskem zakoniku (KZ-1, Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17 in 23/20) in Obligacijskem zakoniku (OZ, Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631), saj je vsebina navadne pošte enako varovana kot vsebina elektronske pošte (Informacijski pooblaščenec, 2019). Drugi odstavek 139. člena KZ-1, ki govori o kršitvi tajnosti občil, določa, da se lahko z

zaporom do enega leta kaznuje vsakogar, ki se z uporabo tehničnih sredstev neupravičeno seznani s sporočilom prenesenim s komunikacijskim sredstvom, prav tako se kaznuje nezakonito posredovanje vsebine sporočil nekomu drugemu. Vsakdo ima od sodišča ali drugega pristojnega organa pravico zahtevati, da se prenehajo ali preprečijo dejanja, ki kršijo nedotakljivost človekove osebnosti, osebnega in družinskega življenja, kar določa 134. člen OZ.

Pomembno je, da so interni pravilniki delodajalcev oblikovani jasno in nedvoumno, v skladu z napredkom IKT, pri čemer mora delodajalec pri določenih omejitvah upoštevati zakonske določbe. Sam interni pravilnik namreč delodajalcu ne dopušča popolne svobode pri oblikovanju pravil, ki bi lahko na primer določala, da se bo uporaba interneta nadzorovala. V internem pravilniku morajo biti pravila uporabe službenih sredstev jasna in določena vnaprej, delodajalec pa mora poskrbeti, da se zaposleni seznanijo z njimi (Karlovšek idr., 2008). V Sloveniji je sam vpogled v vsebino sporočil mogoč zgolj v izjemnih primerih, ko takšen poseg v komunikacijsko zasebnost odredi sodišče, je pa res, da so takšni pogoji za delodajalce precej nepraktični, saj so zahtevnejši za samo dokazovanje in so na nek način neenakovredni delavčevi pravici do zasebnosti (Bečan idr., 2016, str. 262). Takšna določila so precej toga, saj utegne medtem za delodajalca že nastati škoda; v primeru, da bi ta sumil na kaznivo dejanje s strani zaposlenega, pa njegov sum morda ne bi bil dovolj utemeljen oz. bi temeljil zgolj na špekulacijah, ki ne bi bile dovolj podkrepljene za samo sodno odreditev razkritja vsebine sporočil. Dejstvo je, da delodajalec mora imeti pregled nad storilnostjo zaposlenih, seveda pa to ne pomeni, da lahko izvaja nadzor ves čas in v vsakem primeru. Delodajalec na primer lahko omeji zasebno uporabo spleta zgolj za službene potrebe s tem, da blokira dostop do določenih spletnih strani, vendar lahko dopušča zaposlenim zasebno rabo spleta bodisi v času odmora ali če je ta namenjena izobraževanju in napredovanju zaposlenega (Blanpain & Gestel, 2004, str. 48, 50). Bistveno je, da so delodajalci seznanjeni z dejstvom, da je s pomočjo programske opreme nedopustno stalno nadzorovati delavčevo aktivnost na spletu (Mušič, n. d.).

Pomembno je, da se zaposlene (predvsem v storitvenem sektorju) prav tako poduči o pravilnem ravnanju s službeno elektronsko pošto. Elektronska sporočila naj bodo čim krajša, pri čemer je najbolje, da je že v naslovu sporočila razviden predmet dopisovanja. Treba je biti pazljiv tudi pri velikosti priloženih datotek in izogibanju HTML-povezav (Blanpain & Gestel, 2004, str. 39). Delodajalec lahko omeji velikost poštnih predalov oz. nastavi filtre elektronske pošte, ki vnaprej omejujejo velikost priponk elektronske pošte, v primeru, da bi obstajal sum, da zaposleni s svojo aktivnostjo upočasnjujejo strežnike itd., saj se na ta način ne posega v samo vsebino sporočila (Informacijski pooblaščenec, 2019). Nepriporočljivo je že samo odpiranje oz. odgovarjanje na t. i. ''spam'' sporočila, saj je pošiljatelju v takih primerih lahko vidna lokacija prejemnika sporočila, kar lahko še povečuje možnost nezaželenega vdora v sam poštni predal. Če je le možno, naj se zaupna sporočila pošiljajo z

metodo kriptografije, ki omogoča enkripcijo oz. tajnost vsebine (Blanpain & Gestel, 2004, str. 239). Sicer ostajajo elektronska sporočila na strežniku podjetja, dokler niso arhivirana, kar pomeni, da ostajajo na strežniku približno 180 dni (Blanpain & Gestel, 2004, str. 104). Za potrebe poslovanja s strankami je priporočljivo uvesti skupne elektronski predale, npr. info@, stranke@ ipd. (Informacijski pooblaščenec, 2019), predvsem v podjetjih, kjer zaposleni strankam dnevno svetujejo.

Delodajalec mora primere morebitnih posegov v elektronsko pošto oz. možnosti samega nadzora navesti v internem pravilniku, s tem, da kritično presodi, kateri so ti primeri. Tukaj gre za redke in strogo dopustne posege v vsebino sporočil, kot so npr. sum na kaznivo dejanje zaposlenega, ko lahko vsebina korespondence predstavlja dokazno gradivo, ali ko nastane smrt ali daljša odsotnost delavca, podjetje pa podatke oz. dokumentacijo, shranjeno v poštnem predalu zaposlenega nujno potrebuje za nemoteno poslovanje itd. (Informacijski pooblaščenec, 2019). ZDR-1 v prvem in drugem odstavku 10. člena določa, da mora delodajalec vse predloge splošnih aktov, ki vplivajo na delo organizacije oz. zaposlenih, pred samim sprejetjem v pregled posredovati sindikatom in v primeru, da le-ta poda mnenje, ga mora delodajalec upoštevati oz. po potrebi prilagoditi in popraviti. Bistveno je, da so zaposleni dokazljivo vnaprej obveščeni o morebitni možnosti nadzora njihovih komunikacij. Strogo prepovedano je preusmerjanje službene elektronske pošte zaposlenih na drug elektronski naslov (Informacijski pooblaščenec, 2019). Delodajalci ne smejo preusmerjati službene elektronske pošte tako bivših kot trenutno zaposlenih, saj je elektronski naslov opredeljen kot prometni podatek, ta pa se po ZVOP-1 šteje med osebne podatke, ki se lahko obdelujejo le pod točno določenimi pogoji. Prav tako delodajalec nima pravice do vpogleda v vsebino elektronske pošte, četudi bi pridobil geslo neposredno od zaposlenega, oz. bi mu dal le-ta soglasje, saj bi se morale s samim vpogledom v vsebino sporočil strinjati tudi osebe, katerih elektronski naslov je bil udeležen v komunikaciji (Grimšič, 2015). Po prenehanju delovnega razmerja naj se zaposlenim na podlagi 48. člena ZDR-1, ko ne obstaja več pravna podlaga zanj, ukine, oz. onemogoči službeni elektronski naslov, zaposlenim pa se pred tem omogoči pregled poštnega predala, da lahko le-te pomembno dokumentacijo ter elektronske naslove, pomembne za poslovanje organizacije še pravočasno posredujejo delodajalcu. Priporočeno je, da se vsaj za tri mesece po preteku delovnega razmerja uredi avtomatski odzivnik službene elektronske pošte zaposlenega, ki pošiljateljem sporoči, da oseba ni več zaposlena na delovnem mestu. Prav tako je priporočen avtomatski odzivnik v primeru, ko je zaposleni dolgotrajno odsoten z delovnega mesta (bodisi na bolniškem staležu ali na dopustu), s tem, da se predhodno določi oz. navede nadomestni elektronski naslov kontaktne osebe, na katero se lahko pošiljatelji v tem primeru obrnejo, brez navedbe razloga, zakaj je zaposleni odsoten (Informacijski pooblaščenec, 2019).

Odločitev malega senata v primeru Barbulescu proti Romuniji v Sloveniji ni bistveno spremenila že obstoječih pravil, ker ESČP dopušča državam članicam prosto presojo pri ureditvi zakonodaje na področju delodajalčevega nadzora službeno-komunikacijske opreme zaposlenih, vendar pa ta ne sme vsebovati določil, ki bi posameznikom priznavala manjše varstvo pravic, kot jih določa EKČP. Države članice lahko na tem področju torej uredijo zakonodajo nekoliko strožje, zato je pri nas glede na ostale evropske države s 37. členom URS strožje varovana komunikacijska zasebnost. Posebnega zakona, ki bi konkretneje urejal zasebnost na delovnem mestu v Sloveniji, trenutno ni, prav tako v področnih zakonih ni natančno določenih pravil, ki bi urejala delodajalčev nadzor nad preverjanjem internetne aktivnosti zaposlenih. Slovenski delodajalci že v času odločitve malega senata ESČP v primeru Barbulescu niso bili upravičeni neutemeljeno nadzorovati elektronske pošte zaposlenih, vendar pa je bilo pred tem v slovenski sodni praksi takšnih primerov malo. Mali senat ni vzpostavil nove sodne prakse, kot jo je kasneje Veliki senat, zato je bila odločitev le-tega bistveno bolj pomembna za nadaljnjo sodno prakso v Sloveniji. Ker je Slovenija ratificirala EKČP, je zavezana k spoštovanju temeljnih človekovih pravic na svojem ozemlju, zato morajo biti tudi odločitve nacionalnih sodišč v skladu z veljavnimi načeli obstoječe sodne prakse ESČP. Veliki senat ESČP je v primeru Barbulescu proti Romuniji ugotovil, da nacionalna sodišča v Romuniji niso ustrezno zaščitila tožnikove pravice do zasebnosti, zato je državam članicam oz. nacionalnim sodiščem določil strožja pravila presoje med tehtanjem pravice delodajalca in delavca na tem področju. Če bo delodajalec iz neupravičenega razloga, torej neutemeljenega na podlagi zakona in nenujnega za dosego cilja in na prikrit način (ne da bi zaposlene o tem obvestil), izvajal nadzor nad elektronsko pošto zaposlenih, obenem pa vsebino sporočil razkril tretjim osebam, bo v primeru spora pred sodiščem poražen. Nacionalna sodišča morajo na podlagi določil Velikega senata ugotavljati sam obseg in časovni potek nadzora ter presojati ustreznost pravnega varstva zaposlenega, ker pride pri takšnem nadzoru do razkritja osebnih podatkov posameznika. V slovenski zakonodaji neupravičen vpogled v vsebino elektronske pošte sankcionira KZ-1, OZ pa delavcu priznava pravno varstvo pravic. Bistveno je, da delodajalec lahko zaposlenim omeji dostop do spleta ali nastavi filtre elektronske pošte, prav tako lahko omogoča uporabo spleta zaposlenim zgolj v času odmora ali če je le-ta namenjena izobraževanju zaposlenega, vendar pa le-ta v internem pravilniku ne more določiti, da se bo internetna aktivnost zaposlenih v določenem obdobju brez posebnega razloga nadzorovala. Interni pravilniki delodajalcev morajo biti pred samim sprejetjem posredovani sindikatom, običajno pa so v le-teh dopustna določila, da je delodajalec upravičen do nadzora elektronske pošte zaposlenih v primeru suma na kaznivo dejanje, daljše odsotnosti ali smrti delavca, torej v primeru, ko podjetje nujno potrebuje dokumentacijo za nemoteno poslovanje, ali pa ko lahko vsebina sporočil predstavlja dokazno gradivo. Delodajalec ne sme preusmerjati ali prestrezati elektronske pošte zaposlenih, prav tako ne sme nadzorovati vsebine sporočil, četudi bi pridobil geslo neposredno od zaposlenega, ker bi se morale s tem strinjati tudi

druge osebe, udeležene pri dopisovanju. Priporočeno je, da se službeni elektronski naslov po koncu delovnega razmerja ukine, pred tem pa se zaposlenemu omogoči pregled poštnega predala, prav tako je smiselno uvesti avtomatski odzivnik, ki pošiljateljem sporoča kontaktni naslov nadomestne osebe v primeru odsotnosti zaposlenega ali pa da naslovnik elektronskega sporočila ni več zaposlen na delovnem mestu.

5 ZAKLJUČEK

Primer Barbulescu proti Romuniji je odličen pokazatelj, kako lahko prepletanje poklicnega in zasebnega življenja hitro preide v spor. Meja med poklicnim in službenim življenjem je zelo tanka, saj predvsem z porastom tehnologije ljudem dopušča ''prenos'' osebnih zadev tudi na delovno mesto. Tako z vidika temeljnih človekovih pravic, kot odločitve Velikega senata ESČP izhaja dejstvo, da je nemogoče pričakovati, da bo zaposlen v celotnem delavniku popolnoma izključil svoje zasebno življenje. Že sam zasebni telefonski klic med službenim časom ali poslano sporočilo v tem kontekstu pomenita kršitev ločevanja zasebnega in službenega. Kljub temu obstaja razlika med nujnimi zasebnimi zadevami, ki ne morejo počakati, ali občasnim službenim kratkočasenjem, ki lahko vodi do te mere, da poslabša storilnost zaposlenega.

Ko govorimo o delovnem razmerju, ne moremo zanemariti določenih pravil in obveznosti, ki jih je treba na tej točki razmejiti. Že sam ZDR-1 določa, da delavec opravlja delo po navodilih in nadzoru delodajalca. Delodajalec ima legitimno pravico do preverjanja namembnosti službene opreme, dejstvo pa je, da obenem ne sme poseči v interes zaposlenega do pričakovanja zasebnosti, kar je pritrdilo tudi ESČP. Prisotnost interneta v delovnem okolju bo še naprej predstavljala problem marsikateremu delodajalcu, saj se bo ta, kljub morebitni prepovedi uporabe v zasebne namene, izraženi v internem aktu, le stežka prepričal, če je temu res tako. Prav tako je pomembno poudariti, da enotne zakonodaje držav članic o delodajalčevem nadzoru nad službeno-komunikacijsko opremo zaposlenega ni, zato pomanjkanje zakonodaje na tem področju vsekakor vodi do veliko vprašanj, vendar pa je s hitrim napredkom tehnologije tudi nemogoče vnaprej predvideti vsa pravila. Ravno sodba Barbulescuju je tista, ki je delodajalcem še bolj omejila sam vpogled v preverjanje storilnosti zaposlenega, čeprav za Slovenijo iz pravnega vidika ni zavezujoča. Bistveno je, da so države članice seznanjene s sodno prakso ESČP, ki je vsaj z vidika varstva zasebnosti na delovnem mestu še vedno naklonjena delavcem. Slovenija je zavezana k spoštovanju temeljnih človekovih pravic, ker je podpisnica EKČP, zato takšni sodni precedensi predstavljajo nacionalnim sodnikom pomembno odločevalno orodje, saj se predmeti varovanja po EKČP v sodnih postopkih vedno znova interpretirajo in s časom dobijo novo dodano vrednost, ki je morda prej ni bilo.

V diplomskem delu na podlagi prvega raziskovalnega vprašanja, ki se glasi: »Kako lahko delodajalec nadzoruje elektronsko pošto zaposlenega?«, ugotovimo, da lahko delodajalec nadzoruje elektronsko pošto zaposlenega le, če predhodno utemelji namen nadzora, ki mora ustrezati zakonitemu cilju. Predvsem, ker gre za precej invazivno metodo posega v zasebnost, mora delodajalec utemeljiti, da na noben drug način ne more doseči zakonitega cilja, kot z vpogledom v samo vsebino sporočil. Delodajalec mora zaposlene o možnosti nadzora pred samim začetkom dokazljivo obvestiti in obenem zagotoviti, da rezultati

nadzora ne bodo vidni tretjim osebam, če to ni izrecno potrebno. Tukaj gre za izjemne in nujne primere, kot so sum na kaznivo dejanje s strani zaposlenega, vsebina korespondence pa predstavlja dokazno gradivo, smrt ali daljša odsotnost zaposlenega, delodajalec pa dokumentacijo, shranjeno v poštnem predalu nujno potrebuje za nemoteno poslovanje podjetja. Delodajalec ne sme neutemeljeno nadzorovati vsebine korespondence zaposlenega, saj je iz nje možno izslediti tudi posameznikove zasebne zadeve, ki niso vezane na obstoj delovnega razmerja. Ker so osebni podatki vsa dejstva in značilnosti, s katerimi je možno določiti identiteto, oziroma lastnosti posameznika, se torej med osebne podatke posameznika šteje tudi sama vsebina dopisovanja. Osebni podatki posameznika so zgolj v njegovi domeni, razen če njihove obdelave ne določa zakon oz. če sam privoli v obdelavo osebnih podatkov.

Kljub temu da je Veliki senat ugotovil kršitev 8. člena EKČP, se z odločitvijo številni sodniki ESČP niso strinjali, na kar so opozorili tudi v skupnem odklonilnem mnenju. Iz njega izhaja predvsem, da je treba upoštevati delovnopravno zakonodajo in zakonodajo posamezne države članice, prav tako pa so opozorili na dejstvo, da je bilo v primeru nekaj nejasnosti oz. pomanjkanja dokazov. Sodniki Velikega senata so v skupnem odklonilnem mnenju zavzeli stališče, da morajo delovna razmerja temeljiti na obojestranskem zaupanju med delavcem in delodajalcem, tako da ne moremo spregledati dejstva, da je zaposleni s svojim ravnanjem ravno tako ravnal napačno. Bistveno je, da se tako delavci kot delodajalci zavedajo, da nobena od danih pravic ni absolutna. Tako, kot so napačne domneve, da ima delodajalec, ker si lasti službeno opremo, pravico do popolnega nadzora, tako tudi delavec, kljub temu da ga ščiti pravica do zasebnosti na delovnem mestu, zaradi tega ne more pozabiti na določena pravila, ki jih postavlja samo delovno razmerje. V slednjem primeru se je ESČP postavilo na stran delavca, vsekakor pa bo v prihodnosti še vedno prihajalo do konfliktov interesov, saj bodo imeli delodajalci s še bolj omejeno pravico do nadzora manj resničnega vpogleda v dejansko storilnost zaposlenih.

V odgovoru na drugo raziskovalno vprašanje, ki se glasi: »Katera pravila bodo morala nacionalna sodišča v primeru spora med delavcem in delodajalcem na podlagi sodbe Barbulescu proti Romuniji upoštevati in kakšna priporočila so se izoblikovala na podlagi tega primera v zvezi z ravnanjem z elektronsko pošto na delovnem mestu?«, se osredotočamo na pomen sodbe za RS. Sodba je vsebinsko pomembna zato, ker je v Slovenijo na zakonsko pomanjkljivo področje vnesla neko novo sodno prakso, ki je sodišča do tedaj še niso poznala, predvsem z vidika napredka informacijske tehnologije, ki delodajalcem na trgu z nizkimi cenami omogočajo vedno več takšnega ali drugačnega nadzora nad zaposlenimi. Nova sodna praksa sproži nove poglede na pravice in dolžnosti tako delodajalca, kot njegovih zaposlenih, vendar ne smemo pozabiti, da ni dobro, če se poudarjajo samo pravice in dolžnosti ene stranke v delovnem razmerju, temveč vseh udeležencev. Kljub temu da je ESČP v preteklosti že obravnavalo primere pričakovane zasebnosti na delovnem mestu, gre

v slednjem primeru za razvoj sodne prakse na novem področju – nadzor nad elektronsko pošto oz. nadzor nad internetno aktivnostjo zaposlenega, za katero je Veliki senat ESČP presodil, da je zaradi hitrih sprememb na področju razvoja IKT nujna. Nedvomno so tako odmevne sodbe medijsko prisotne, zato je tudi ta vzbudila veliko zanimanje javnosti. Na eni strani so stališča informacijskega pooblaščenca, ki se z odločitvijo Velikega senata strinja, na drugi strani pa so delodajalci, ki bodo zaradi slednje sodbe bistveno bolj omejeni pri preverjanju storilnosti službenih opravil zaposlenih. Nacionalna sodišča držav članic morajo na podlagi slednjega primera pri svoji presoji ob morebitnem sporu med delodajalcem in delavcem v zvezi z nadzorom elektronske pošte ugotavljati in upoštevati, ali je bil delavec vnaprej dokazljivo obveščen s strani delodajalca o možnosti nadzora, ali so bili spremljani zgolj prometni podatki ali tudi sama vsebina korespondence ter kdo je imel dostop do rezultatov nadzora oz. teh podatkov. Če delodajalec upravičeno utemelji svoj namen nadzora, je do rezultatov nadzora upravičen zgolj sam ali oseba, ki jo za to pooblasti, nikakor pa ne sme biti vsebina sporočil vidna ostalim, za to neupravičenim osebam. Nacionalna sodišča morajo prav tako pretehtati posledice nadzora, ki jih je sam nadzor nad vsebino sporočil prinesel delavcu, ter ugotoviti dejstvo, ali je imel delavec na voljo ustrezno pravno varstvo, ko je prišlo do nadzora, torej možnost pritožbe zoper obdelave osebnih podatkov itd. Seveda bo treba še vedno za vsak primer posamezno opredeliti, kateri interes bo prevladal, vendar se bodo nacionalna sodišča v podobnih primerih opirala ravno na postopek primera Barbulescu proti Romuniji, kot se je v Sloveniji že npr. Višje delovno sodišče leta 2018, sodba pa daje na nek način delojemalcem občutek, kot da jim delodajalec pri opravljanju dela po novem skoraj ''nič ne more''. Po drugi strani je tudi Uredba GDPR v slovensko zakonodajo posameznikom prinesla bistveno več pravic in varoval v zvezi z obdelavo osebnih podatkov, zato je to področje precej strožje urejeno, kot je bilo v preteklosti. Vendar pa se v zvezi z delodajalčevim nadzorom kljub temu poraja vprašanje, kakšen je sploh pomen le-tega, če bodo zaposleni pred tem vedno obveščeni, saj se na ta način težje odkrije oz. prepreči morebitna škodljiva dejanja. Ker mora delodajalec svoj namen nadzora po odločitvi Velikega senata ESČP vedno utemeljiti, utegne že pred samo uvedbo nadzora za delodajalca nastati škoda, saj je utemeljitev suma na kaznivo dejanje težje dokazovati. Takšna določila so za delodajalca precej nepraktična, zato delodajalčeva lastninska pravica nad opremo na nek način ni enakovredna delavčevi pravici do zasebnosti. V delovnem razmerju se delodajalcem na podlagi slednje sodbe v zvezi z ravnanjem z elektronsko pošto priporoča, naj delavcem v prvi vrsti naročijo ločevanje službene in zasebne elektronske pošte, po preteku delovnega razmerja pa naj se le-ta ukine. Priporočeno je tudi, da se za potrebe poslovanja s strankami uvedejo skupni elektronski predali, npr. @info ipd., ter omeji velikost poštnih predalov ali določi filtre. Kot nedopustno se šteje preusmerjanje elektronske pošte na drug naslov, prav tako je nedopustno nadziranje elektronske pošte s pomočjo programske opreme ali s pridobitvijo gesla, četudi neposredno od zaposlenega. Pomembno je tudi, da so že sami interni pravilniki

delodajalcev oblikovani v skladu z zakonodajo, kjer je na primer nedopustno določiti, da se bo komunikacija zaposlenih lahko nadzorovala, prav tako je priporočljivo, da se zaposlene, predvsem v storitvenem sektorju, poduči o pravilnem ravnanju s službeno elektronsko pošto.

Dejstvo je, da se bo informacijska tehnologija razvijala še naprej, čemur bo moralo slediti tudi delovno pravo. Glede na to, da v slovenski zakonodaji ni natančno določenih pravil glede delodajalčevega nadzora nad službeno-komunikacijsko opremo zaposlenih, bi bilo to smiselno urediti na način, da bi se uvedla pravila, ki bi na eni strani ne samo ščitila interese zaposlenih, temveč zaščitila tudi interese delodajalcev. Že sama omemba nadzora v delovnem okolju bi dosegla svoj namen, če bi le-ta pripomogel k boljši ozaveščenosti zaposlenih, da morajo ločiti službene in zasebne zadeve. Četudi do samega zakona o zasebnosti na delovnem mestu v prihodnosti ne bo prišlo, bi konkretnejša določila o delodajalčevem nadzoru službeno-komunikacijske opreme lahko urejal ZDR-1, kot sedaj že vsebuje posebna določila za videonadzor in biometrijo. Ker takšni nadzori niso nov pojem, so bile v preteklosti na tem področju že izvedene mnoge raziskave o tem, kako uvedba delodajalčevega nadzora vpliva na storilnost zaposlenih, ali se zaposleni zavedajo svojih pravic v zvezi z varovanjem osebnih podatkov v delovnem razmerju itd., v diplomskem delu pa smo bili osredotočeni na aktualen primer iz sodne prakse ESČP, zato bi bilo v prihodnje smiselno spremljati statistiko pritožb pri informacijskem pooblaščencu zoper kršitve obdelave osebnih podatkov v delovnem razmerju, obenem pa raziskati, kako bi po drugi strani delodajalcem omogočali pravno varstvo ob zlorabi prepovedi uporabe službeno-komunikacijske opreme v zasebne namene s strani zaposlenih.

LITERATURA IN VIRI

LITERATURA

Armič, D. (2013). *Pravica do zasebnosti v sodni praksi Evropskega sodišča za človekove pravice* (diplomsko delo). Maribor: Univerza v Mariboru, Fakulteta za zdravstvene vede. Pridobljeno s https://dk.um.si/Dokument.php?id=54890

Bečan, I., Belopavlovič, N., Horvat, E. K., Kresal, B., Šoltes, K. K., Mežnar, Š., . . . Tekavc, M. Š. (2016). *Zakon o delovnih razmerjih (ZDR-1) s komentarjem.* Ljubljana: Narodna in univerzitetna knjižnica.

Blanpain, R. & Gestel, M. V. (2004). *Use and monitoring of E-Mail, Intranet and Internet Facilities at Work.* The Hague; London; New York: Kluwer Law International.

Brajnik, M. (5. 8. 2019). *Nadzor zaposlenih na delovnem mestu*. Pridobljeno s https://www.iusinfo.si/medijsko-sredisce/v-srediscu/247067

Brdnik, V. (2016). *Pomen človekovih pravic in izvrševanje sodb ESČP* (diplomsko delo). Kranj: Nova Univerza - Fakulteta za državne in evropske študije.

Cvetko, A. (1999). *Varovanje zasebnosti v delovnih razmerjih*. Ljubljana: Gospodarski vestnik.

Černič, J. L. (23. 3. 2012). *Sodbe Evropskega sodišča za človekove pravice kot nebodigatreba obveznost.* Pridobljeno s https://www.iusinfo.si/medijsko-sredisce/kolumne/79975

Dashöfer, V. (13. 2 2018). *Odgovori na najpogostejše dileme o GDPR.* Pridobljeno s https://www.varstvo-podatkov.si/33/odgovori-na-najpogostejse-dileme-o-gdpr-uniqueiduchxzASYZNafRpJK1--koPIgrYgrFmPu/

Djinović, M. (2018). *Vse, kar morate vedeti o privolitvi za obdelavo osebnih podatkov.* Pridobljeno s https://www.gzs.si/Portals/SN-informacije-Pomoc/Vsebine/GG/2018-april/26-27-GDPR.pdf

Drozg, I. (4. 4. 2015). *Ali je dovoljeno zaposlene elektronsko nadzirati?* Pridobljeno shttp://www.racunovodski-servis-zeus.si/aktualne-informacije/e-nadzor-zaposleni

Fakin, A. (11. 1. 2019). *Miti o GDPR*. Pridobljeno s https://www.aljafakin.si/miti-o-gdpr/

Feguš, P. (b. d.). *Pravne prakse nadzora nad zaposlenimi*. Pridobljeno s https://www.hrm-revija.si/pravne-prakse-nadzora-nad-zaposlenimi

Franca, V. (7. 2. 2010). *Strahovi in izzivi socialnih omrežij v kadrovski dejavnosti*. Pridobljeno s http://ecg.si/clanki/strahovi-in-izzivi-socialnih-omrezij-v-kadrovski-dejavnosti/

Gogala, M. (2015). *Slovenija pred Evropskim sodiščem za človekove pravice* (magistrsko delo). Nova Gorica: Nova Univerza - Evropska pravna fakulteta.

Gomien, D. (2009). *Kratek vodič po Evropski konvenciji o človekovih pravicah.* Ljubljana: Ministrstvo za pravosodje, Center za izobraževanje v pravosodju.

Grimšič, M. B. (17. 9. 2015). Preusmeritev elektronske pošte bivšega zaposlenega prepovedana. Pridobljeno s https://data.si/blog/preusmeritev-elektronske-poste-bivsega-zaposlenega-prepovedana/

Havliček, M. (1. 6. 2012). *E-pošta in zasebnost na delovnem mestu*. Pridobljeno s https://eudace.eu/knjiznica/clanki/2013021410315019/

Jacksteit, T. T. (2019). *Analiza varstva osebnih podatkov po predlogu ZVOP-2* (diplomsko delo). Maribor: Univerza v Mariboru, Fakulteta za varnostne vede. Pridobljeno s https://dk.um.si/Dokument.php?id=137044

Jamšek, B. (20. 11. 2018). GDPR: *Uredba o varstvu podatkov*. Pridobljeno s https://mladipodjetnik.si/novice-in-dogodki/novice/gdpr-uredba-o-varstvu-podatkov

Karlovšek, S. B., Jerše, A., Mišič, K., Musar, N. P., Rupnik, J. & Tomšič, A. (2008). *Zasebnost delavcev in interesi delodajalcev – kje so meje?* Ljubljana: Uradni list RS.

Klemenčič, G. (2002). *Človekove pravice in temeljne svoboščine / 37. člen; Področje varovanja.* Pridobljeno s https://e-kurs.si/komentar/podrocje-varovanja-9/

Kovačič, M. (2006). *Nadzor in zasebnost v informacijski družbi.* Ljubljana: Znanstvena knjižnjica Fakultete za družbene vede.

Lampe, R. (2004). Mednarodnopravni vidiki pravice do zasebnosti- jurispudenca 8. člena Evropske konvencije o človekovih pravicah in temeljnih svoboščinah. *Pravnik: revija za pravno teorijo in prakso*, *59*(7/9), 196-227.

Makarovič, B., Možina, D., Mežnar, Š., Bizjak, D., Bogataj, M. & Klemenčič, G. (2003). *Internet in pravo.* Ljubljana: Pravna fakulteta.

Mikuž, D. (2017). P*roblematika ureditve varstva osebnih podatkov delavcev* (magistrsko diplomsko delo). Ljubljana: Univerza v Ljubljani, Pravna fakulteta. Pridobljeno s https://repozitorij.uni-lj.si/Dokument.php?lang=slv&id=108790

Mušič, T. K. (b. d.). *Vpliv primera Barbulescu proti Romuniji na Slovenske delodajalce*. Pridobljeno s https://pirc-musar.si/sl/vpliv-primera-barbulecsu-proti-romuniji-na-slovenske-delodajalce/

Pirc Musar, N. (2006). *V sožitju javnosti in zasebnosti.* Pridobljeno s https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/zasebnoNIjavno_slo.pdf

Pirc Musar, N. (11. 7. 2014). Ena najpomembnejših zmag: Hramba prometnih podatkov je v Sloveniji neustavna. *Dnevnik*. Pridobljeno s https://www.dnevnik.si/1042673965

Prelesnik, M. (2017). *Zasebnost na delovnem mestu*. Pridobljeno s https://www.sviz.si/datot/zasebnost-na-dm-seminar2017.pdf

Prelesnik, M. (6. 3. 2020). *Novi predlog uredbe o e-zasebnosti bistveno niža raven varstva pravic posameznikov pri uporabi elektronskih komunikacij in na široko odpira vrata posegom v pravice zaradi poslovnih interesov ponudnikov storitev*. Pridobljeno s https://www.ip-rs.si/novice/novi-predlog-uredbe-o-e-zasebnosti-bistveno-niza-raven-varstva-pravic-posameznikov-pri-upo-1166/

Štampar, A. S. (16. 6. 2019). Pravno normiranje korporativnega upravljanja. *DIGNITAS Revija za človekove pravice Slovenian journal of human rights,* 73/74, 87–112.

Teršek, A. (13. 12. 2008). Sodobna koncepcija socialne države presega klasično. *Dnevnik.* Pridobljeno s https://www.dnevnik.si/1042229310

Teršek, A. (2018). *Etika politike; Esejistični komentar ustave z novo ustavo.* Ljubljana: UMco.

Unit, P. (5. 9. 2017). *Q & A Grand Chamber judgment in the case of Bărbulescu v. Romania (application no. 61496/08)*. Pridobljeno s https://www.echr.coe.int/Documents/Press_Q_A_Barbulescu_ENG.PDF

Zupančič, L. (8. 1. 2015). Meja dopustnega nadzora nad uporabo interneta in elektronske pošte na delovnem mestu. *Pravna praksa PP: časopis za pravna vprašanja*, *34*(1), 2–7.

Žgur, M., Šalamon, N. K. & Koritnik, B. (19. 7. 2017). *Challenges of the Constitutional Law in the 21st Century - Liber Amicorum Ciril Ribičič.* Pridobljeno s file:///C:/Users/rebek/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/53-Book%20Manuscript-202-1-10-20170719%20(1).pdf

VIRI

Brosix. (13. 4. 2020). *7 Reasons to Use a Work Instant Messenger*. Pridobljeno s https://www.brosix.com/blog/work-instant-messenger/

European Court of Human Rights. (12. 1. 2016). *CASE OF BARBULESCU V. ROMANIA*. Pridobljeno s https://hudoc.echr.coe.int/rus#{"itemid":["001-159906"]}

European Court of Human Rights. (5. 9. 2017). *CASE OF BĂRBULESCU v. ROMANIA*. Pridobljeno s https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-177082%22]}

European Court of Human Rights. (31. 8. 2019). *Guide on Article 8 of the European ConventiononHuman Rights.* Pridobljeno s https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

Evropska komisija. (b. d.). *Vrste predpisov EU.* Pridobljeno s https://ec.europa.eu/info/law/law-making-process/types-eu-law_sl

ILO. (1997). Protection of worker's personal data. *An ILO code of practice*. Pridobljeno s https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

ILO. (6. 4. 2020). *How the ILO works*. Pridobljeno s http://www.ilo.org/global/about-the-ilo/how-the-ilo-works/lang--en/index.htm

Informacijski pooblaščenec. (25. 11. 2019). *Varstvo osebnih podatkov v delovnih razmerjih, smernice Informacijskega pooblaščenca.* Pridobljeno s https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_-_Varstvo_OP_v_delovnih_razmerjih_verzija_1.1_koncna.pdf

Informacijski pooblaščenec. (b. d.). *Pooblaščena oseba za varstvo osebnih podatkov.* Pridobljeno s https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/pooblascena-oseba-za-varstvo-podatkov/#c1906

Jadek & Pensa. (23. 10. 2017). *Zasebnost na delovnem mestu – Delodajalci, pozor pri nadzoru elektronskih komunikacij delavca!* Pridobljeno s https://www.jadek-pensa.si/zasebnost-na-delovnem-mestu-delodajalci-pozor-pri-nadzoru-elektronskih-komunikacij-delavca/

Ministrstvo za pravosodje. (5. 11. 2019). *Izvrševanje sodb Evropskega sodišča za človekove pravice in priporočil Varuha človekovih pravic*. Pridobljeno s https://www.gov.si/podrocja/pravna-drzava-in-pravosodje/izvrsevanje-priporocil-varuha-in-sodb-evropskega-sodisca-za-clovekove-pravice/

Ministrstvo za zunanje zadeve RS. (2015). Mednarodna organizacija dela. Pridobljeno s http://www.zeneva.predstavnistvo.si/index.php?id=2487

PeoplePill. (b. d.). *Ayşe Işıl Karakaş.* Pridobljeno s https://peoplepill.com/people/ayse-isil-karakas/

Sistema penale. (6. 11. 2019). P*aulo Pinto De Albuquerque.* Pridobljeno s https://www.sistemapenale.it/it/autori-di-sp/pinto-de-albuquerque-paulo

Služba Vlade Republike Slovenije za zakonodajo. (2018). *Nomotehnične smernice.* Pridobljeno s https://www.gov.si/assets/vladne-sluzbe/SVZ/f50d0f6d15/Nomotehnicne_smernice-2018.pdf

Služba Vlade Republike Slovenije za zakonodajo. (17. 4. 2019). *Temeljni akti Republike Slovenije.* Pridobljeno s https://www.gov.si/teme/temeljni-akti-republike-slovenije/

SPIRIT Slovenija. (27. 8. 2019). *Nadzor zaposlenih na delovnem mestu*. Pridobljeno s https://www.podjetniski-portal.si/moj-spletni-prirocnik/22641-nadzor-zaposlenih-na-delovnem-mestu

STA. (4. 3. 2020). *V nastajanju evropska uredba o e-zasebnosti*. Pridobljeno s https://www.iusinfo.si/medijsko-sredisce/v-srediscu/258565

Urad Vlade Republike Slovenije za komuniciranje. (6. 12. 2019). *Ustavno sodišče.* Pridobljeno s https://www.gov.si/drzavni-organi/ustavno-sodisce/

PRAVNI VIRI

Ustava Republike Slovenije (URS). Uradni list RS, št. od 33/91-I do 75/16 – UZ70a.

Evropska konvencija o človekovih pravicah in temeljnih svoboščinah, Zakon o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11. Uradni list RS – Mednarodne pogodbe, št. 7/94.

Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24.10.1995 o varstvu posameznikov pri obdelavi osebnih podatkov in prostem pretoku takih podatkov. Uradni list EU, št. 182 z dne 23.11.1995.

Kazenski zakonik (KZ-1). Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17 in 23/20

Obligacijski zakonik (OZ). Uradni list RS, št. 97/07 – uradno prečiščeno besedilo, 64/16 – odl. US in 20/18 – OROZ631

Zakon o delovnih razmerjih (ZDR-1). Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS in 81/19.

Zakon o elektronskih komunikacijah (ZEKom-1). Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17.

Zakon o varstvu osebnih podatkov (ZVOP-1). Uradni list RS, št. 94/07 – uradno prečiščeno besedilo)