VARSTVO DELAVČEVE INFORMACIJSKE ZASEBNOSTI

Andrej Tomšič*

UDK: 349.2:343.45

Povzetek: *V informacijski družbi je zasebnost pogosto na udaru, pritiske na zasebnost pa stopnjuje hiter tehnološki napredek in zaostajanje pravne ureditve. Zasebnost na delovnem mestu je predmet konflikta interesov in pravic delodajalca, zaposlenih in tretjih oseb ter področje, kjer se soočamo z izrazito pravno podnormiranostjo. V prispevku so prikazane razlike v ureditvi zadevnega področja med ZDA in EU, primeri sodne prakse ter pravna ureditev v Sloveniji. Ob odsotnosti zakonodaje, ki bi natančneje uravnovesila pravice in interese delodajalca in zaposlenih, je treba poskrbeti za transparentno interno ureditev ob upoštevanju ustavnih in zakonskih norm.*

Ključne besede: *informacijska zasebnost, varstvo osebnih podatkov, utemeljenost pričakovanja zasebnosti, sodna praksa, zasebnost na delovnem mestu*

PROTECTION OF WORKERS' INFORMATION PRIVACY

Abstract: *Privacy in the information society is facing many pressures, which are even enhanced by rapid technological development and the lagging behind of legal response. Workplace privacy is a matter of conflict of interests between the employer, the employees and third parties and is as such an area of apparent legal void. The article shows the differences in workplace privacy between US and the EU; it advocates the adoption of transparent provisions in internal regulations to balance the interests*

* Andrej Tomšič, magister poslovnih ved, namestnik informacijske pooblaščenke, Informacijski pooblaščenec Republike Slovenije
andrej.tomsic@ip-rs.si
Andrej Tomšič, Msc., Deputy Information Commissioner, Information Commissioner of the Republic of Slovenia.

of the employer and employees until particular legislation in this field is adopted.

Key words: *Information privacy, personal data protection, reasonable expectation of privacy, case-law, workplace privacy*

1. UVOD

Namesto uvoda za trenutek pomislimo na nekaj praktično vsakdanjih dogodkov, ki jim zaposleni ob opravljanju rednih delovnih nalog neizogibno namenijo del časa. Zaposleni se ob jutranji kavi s sodelavci pogovarja o službenih in zasebnih zadevah. S službenega telefona v pisarni pokličemo partnerja, da se dogovorimo, kdo bo šel danes po otroka v vrtec. Po kosilu preverimo novice na spletnih straneh in pogledamo, ali smo dobili kakšno sporočilo v zasebni predal elektronske pošte.

Verjetno bi težko našli posameznika, ki ni nikoli v okviru delovnega časa storil niti enega od navedenih dejanj – upam si trditi celo, da težko najdemo posameznika, ki ne počne večine od navedenih dejanj. To seveda še ne pomeni nujno, da to počne velik del delovnega časa, določen del delavnika pa se gotovo nameni tudi aktivnostim, ki niso neposredno povezane z opravljanjem delovnih zadolžitev in nalog. V času informacijske družbe je zanimiva razlika ta, da so sodobne tehnologije, kot so internet, elektronska pošta in pametni telefoni, v določeni meri zamenjali bolj tradicionalne medije in metode za neproduktivno izrabo delovnega časa – branje tiskanih časopisov, odmore za kavo in cigarete itd. Zaposleni namreč ne prej ne sedaj nismo bili roboti in smo vedno – pa čeprav se tega nismo dobro zavedali – pričakovali določeno, pa čeprav omejeno raven zasebnosti tudi na delovnem mestu.

Če imamo torej na strani posameznika kot zaposlenega dejansko stanje, ki se ga praktično vsi zavedamo, imamo na drugi strani delodajalca, katerega interesi, pravice in dolžnosti so pogosto v konfliktu z interesi zaposlenega. Oglejmo si nekaj konkretnih primerov. Zaposleni ima zelo visoke račune za službeni mobilni telefon. Delodajalec sumi, da zaposleni izdaja interne informacije, komunicira z določenimi mediji ali celo izdaja tajne podatke. Predstojnik organa meni, da zaposleni pretirano uporabljajo dostop do interneta in da preveč časa »visijo« na Facebooku in podobnih spletnih straneh. Vodja informatike preverja, ali zaposleni po službeni elektronski pošti pošiljajo zabavne filmčke. Minister želi ugotoviti,

kdo od zaposlenih je določen dokument, ki naj bi vseboval zaupne podatke, posredoval medijem, predsednik sodišča pa želi vedeti, kdo po telefonu komunicira z določenimi novinarji, in odredi pridobitev podatkov in nadzor nad opravljenimi telefonskimi klici. Vse to so situacije, s katerimi se je že srečal Informacijski pooblaščenec kot nadzorni organ za varstvo osebnih podatkov.

Zelo očitno je torej, da gre za konflikt interesov delodajalca in zaposlenih. Prvi utemeljeno pričakuje, da zaposleni ne bodo uporabljali službene opreme za dejanja, ki predstavljajo kršitev konkurenčnih prepovedi, za dejanja, ki predstavljajo disciplinske kršitve oz. prestopke, ter za zlorabo službenih sredstev v zasebne namene. Pričakovanja delodajalca izhajajo iz njegove lastninske pravice, iz katere izhaja tudi njegova pravica do nadzora nad uporabo službenih sredstev in ravnanjem zaposlenih. Zaposleni na drugi strani utemeljeno pričakujejo, da bo delodajalec spoštoval pravico delavca do zasebnosti na delovnem mestu, da bo spoštoval njegovo dostojanstvo, integriteto in druge osebnostne pravice. Zaposleni zato pričakuje, da lahko tudi na delovnem mestu pričakuje določeno stopnjo zasebnosti, da s prečkanjem praga delodajalca ne postaja popolnoma nadzorovani robot in da bo vnaprej obveščen o tem, kaj in v kolikšni meri lahko uporablja v zasebne namene ter kdaj, pod kakšnimi pogoji in v kakšnih okoliščinah bo uporaba določenih sredstev tudi nadzorovana.

Konflikt med interesi omenjenih dodatno zaostrita še dva pomembna faktorja.

Prvič, pri zasebnosti na delovnem mestu nimamo samo dveh strank, katerih interesi so v konfliktu, temveč imamo pogosto tudi tretje osebe, ki imajo prav tako svoje interese in uživajo določene pravice. Zaposleni namreč vsakodnevno komuniciramo z osebami izven svojega delovnega okolja, in s tem, ko delodajalec nadzira komunikacijo zaposlenega (telefon, elektronsko pošto ipd.), nadzira tudi tretje osebe in njihovo komunikacijo z zaposlenimi. Če delodajalec lahko do neke mere obvesti zaposlene o tem, katera službena sredstva so podvržena nadzoru in pod kakšnimi pogoji, kako lahko o tem obvesti tretje osebe, ki zaposlenega kličejo ali mu pošiljajo elektronsko pošto tudi povsem zasebne narave?

Drugič, intenzivnost in obseg navedenega konflikta sta v informacijski družbi potencirana s sodobnimi načini komuniciranja ter hrambe in obdelave podatkov. Danes je mogoče prek spleta naročiti program, ki omogoča skoraj vse, kar si lahko zamislimo glede nadzora uporabe računalnika s strani zaposlenih – beleži vse, kar zaposleni počne na računalniku: obiskane spletne strani, poslano in prejeto e-pošto s priponkami, vsebino pogovorov pri neposrednem sporočanju. Direktor ali predstojnik lahko v živo spremlja, kaj zaposleni trenutno počne na

računalniku – na kateri spletni strani se nahaja, komu piše e-pošto, kaj tipka v urejevalniku besedil. Nadzor nad zaposlenimi je s tehnološkega vidika enostaven, učinkovit in poceni.

2. PRAVNA UREDITEV V ZDA IN EU

Ureditev vprašanja zasebnosti na delovnem mestu v ZDA se precej razlikuje od ureditve tega vprašanja v evropskem prostoru. Bistvo razlik v odločitvah sodnih organov se nanaša na odnos do zasebnosti na delovnem mestu in pravice lastnine nad službenimi sredstvi in osebnimi podatki, ki pri tem nastajajo oziroma se obdelujejo. Sodišča v ZDA tako dajejo večji poudarek pravici do lastnine, in posledično nadzora nad njo, evropska sodna praksa pa predpostavlja tehtanje pravic in vzpostavlja določene minimalne varovalke, ki ščitijo zasebnost zaposlenih na delovnem mestu pred neomejenim nadzorom s strani delodajalca.

2.1. Pravna ureditev in sodna praksa v ZDA

Delodajalci v ZDA večinoma nasprotujejo državni regulaciji zaščite zasebnosti na delovnem mestu in menijo, da zadostuje samoregulacija s strani podjetij.[1] V ZDA je prostorska, komunikacijska in informacijska zasebnost zunaj doma in zunaj konteksta vladnega preiskovanja in zaplembe slabo varovana.[2] Delodajalci v ZDA, kot ugotavlja raziskava American Management Association, čedalje bolj pogosto posegajo v zasebnost svojih zaposlenih, to pravico pa naj bi jim dalo lastništvo nad delovno opremo.[3] Odločitve ameriških sodišč kažejo, da država njihovo početje legitimira, tehnološki razvoj pa omogoča uporabo novih in čedalje cenejših nadzornih naprav. Sodna praksa v ZDA kaže na to, da lahko delodajalec s strani zaposlenega zakonito zahteva podpis soglasja za nadzor v kakršnemkoli obsegu. Tako je v primeru *Bonita P. Bourke, et. al. proti Nissan Motor Corporation* kalifornijsko prizivno sodišče razsodilo, da vpogled v elektronsko sporočilo, ki ga je uslužbenka poslala po omrežju podjetja, ne pomeni neupravičenega vdora v njeno zasebnost, ker je uslužbenka predhodno podpi-

[1] Kovačič, 2006, str. 58.
[2] Cate, 1997, str. 65.
[3] American Management Association/ePolicy Institute Research, 2001, 2005 in 2007.

sala izjavo, v kateri se je zavezala, da bo elektronsko pošto uporabljala zgolj v službene namene.[4] V primeru *Billa McLarena proti Microsofu* iz leta 1999 pa je šlo isto sodišče še dlje. V tem primeru je šlo za to, da je podjetje pregledalo šifrirano elektronsko pošto zaposlenega (ki so jo pred tem seveda dešifrirali), shranjeno v računalniku v mapi "Osebni imenik", zaradi česar je zaposleni sprožil sodni spor. Sodišče je v razsodbi dalo prav delodajalcu, in sicer z obrazložitvijo, da je interes delodajalca, da prepreči pošiljanje neprimerne elektronske pošte, nad interesom zaposlenega do zasebnosti.[5]

2.2. Pravna ureditev in sodna praksa v evropskem prostoru

V Evropi so sodišča, kar zadeva zasebnost komunikacij na delovnem mestu, bolj naklonjena zaposlenim kot v ZDA.[6] Vzpostavila se je namreč sodna praksa, ki narekuje, da načeloma velja obveznost delodajalca, da zaposlene vsaj obvesti o možnosti nadzora na delovnem mestu. V zvezi z nadzorom na delovnem mestu sta najbolj znani odločitvi Evropskega sodišča za človekove pravice (ESČP) v primerih *Halford proti Veliki Britaniji* iz leta 1997[7] v zvezi s kršitvijo 8. člena Evropske konvencije o človekovih pravicah (EKČP) in odločitev v primeru *Copland proti Veliki Britaniji.*[8]

V primeru *Copland v. Združeno kraljestvo* je delodajalec nadzoroval uporabo telefona, in sicer z analizo telefonskih računov, ki je razkrila klicane telefonske številke, datum in čas klicev, njihovo trajanje ter stroške; uporabo interneta preko analize obiskanih spletnih strani, ki je razkrila datum, čas in trajanje obiskov; ter uporabo elektronske pošte na delu preko analize elektronskih naslovov poslanih sporočil ter datuma in časa pošiljanja elektronskih sporočil. V času, ko se je to dogajalo, delodajalec ni imel vzpostavljenih nobenih uradnih pravil glede nadzora telefona, elektronske pošte ali uporabe interneta s strani zaposlenih. V skladu z ustaljeno sodno prakso ESČP sodijo telefonski klici iz službenega mesta v okvir zasebnega življenja in dopisovanja v smislu prvega odstavka 8. člena EKČP. ESČP je v tem primeru odločilo, da v skladu s tem 8. člen ščiti tudi elektronska sporočila, poslana na delovnem mestu, ter informacije, pridobljene

[4] Klemenčič, 2003, str. 137.
[5] Prav tam, str. 137.
[6] Prav tam, str. 137.
[7] *Halford proti Veliki Britaniji*, 25. 6. 1997, Reports, 1997-III.
[8] *Copland proti Veliki Britaniji*, 3. 4. 2007, Appl. No. 62617/00.

z nadzorom osebne uporabe interneta. Pritožnica v tem primeru ni bila opozorjena, da bodo njeni klici predmet nadzora, zato je imela razumna pričakovanja glede zasebnosti klicev iz telefona na delovnem mestu. Enaka pričakovanja veljajo glede elektronske pošte in uporabe interneta. Sodišče je zavzelo stališče, da delodajalec ni imel pristojnosti, da v tem smislu v okviru svojih pristojnosti ukrene »vse potrebno ali primerno« za namene opravljanja dela (v tem primeru zagotavljanja višjega in nadaljnjega izobraževanja), pri čemer v času dogodka ni obstajala zakonska podlaga, ki bi urejala okoliščine, ko delodajalec lahko nadzoruje uporabo telefona, elektronske pošte in interneta zaposlenih.[9]

Med novejšo sodno prakso velja izpostaviti odločitve ESČP v primeru *Köpke proti Nemčiji*[10] in v primeru *Bărbulescu proti Romuniji*.[11] V primeru *Köpke proti Nemčiji* je šlo za namestitev prikritega videonadzora za dokazovanje kraje. Sodišče je ocenilo, da je takšen nadzor lahko pod določenimi pogoji tudi zakonit, in sicer če obstoji utemeljen sum storitve kaznivega dejanja s strani zaposlenega, če tega suma ni mogoče preveriti drugače ali vsaj ne brez velikih stroškov, naporov ali porabe časa, če se nadzor časovno, prostorsko in glede izpostavljenih oseb ustrezno omeji, uporaba posnetkov mora biti omejena izključno za obravnavo navedenega kaznivega dejanja (v disciplinskem postopku/sodnem postopku). Namen prikritega nadzora sme biti le v preiskavi konkretnega in resnejšega incidenta, npr. dlje časa trajajoče evidentne kraje zaposlenih.

V odmevnem primeru *Bărbulescu proti Romuniji* je šlo za nadzor uporabe orodja za sprotno komuniciranje (Yahoo Messenger), ki je bilo namenjeno za odgovore strankam. Zaposleni je bil jasno vnaprej obveščen o prepovedi uporabe računa za zasebne namene, a ga je kljub temu uporabljal za zasebno klepetanje z bratom in zaročenko. ESČP je v konkretnem primeru presodilo, da je bil nadzor delodajalca upravičen, kar so številni domači in tuji mediji žal pretirano posplošili, češ da je takšen nadzor sedaj vedno dopusten in da zaposleni od te sodbe naprej ne morejo pričakovati zasebnosti na delovnem mestu. Sodbe seveda ni primerno posploševati, saj gre vendarle za zelo specifične okoliščine. Med drugim je pomembno to, da je zaposleni delodajalcu predložil pisno izjavo, da je klepetalnik uporabljal samo v službene namene; nadzor delodajalca je bil zato pričakovan in razumen. Pri tem velja opozoriti na nekaj nejasnosti glede dejan-

[9] Glej tudi Informacijski pooblaščenec, neobvezno mnenje št. 0712-228/2008/2 z dne 11. 3. 2008.
[10] *Köpke proti Nemčiji*, 5. 10. 2010, št. 420/07.
[11] *Bărbulescu proti Romuniji*, 12. 1. 2016, št. 61496/08.

skega stanja, saj iz sodbe ni razvidno, kakšen je bil povod delodajalca, da je pridobil izpis komunikacij; sodba je prav tako lahko še predmet obravnave pred Velikim senatom ESČP.

Glede sodne prakse v posameznih državah članicah EU velja izpostavili sodbe Kasacijskega sodišča v Franciji, in sicer zlasti v primerih *Societe Nikon France, SA proti Onof*, 2001, št. 99–42.942, *Bruno B proti Giraud et Migot*, 2009, št. 07-44264 ter *M. X. proti Young & Rubicam France*, 2013, št. 12-12.138. Kasacijsko sodišče je od relativno strogih stališč v prid zaposlenim iz primera *Onof* (2001), s sodbama *Bruno B proti Giraud et Migot* ter *M. X. proti Young & Rubicam France*, svoja stališča nekoliko omililo v smeri utemeljenosti pričakovanja zasebnosti – zaposleni, ki ni ničesar aktivno storil, da bi zavaroval svojo zasebnost na delovnem mestu oziroma z vidika uporabe službenih sredstev (npr. premaknil oziroma označil zasebnih sporočil in dokumentov v ustrezno označeno mapo), v tem delu ne more utemeljeno pričakovati zasebnosti.

3. PRAVNA UREDITEV V SLOVENIJI IN IZKUŠNJE V PRAKSI

Področje zasebnosti na delovnem mestu sodi v okvir delovno-pravne zakonodaje in zakonodaje varstva osebnih podatkov. Nekatere teme, kot so pogoji za uvedbo videonadzora na delovnih mestih ter izvajanje biometrijskih ukrepov nad zaposlenimi, konkretno ureja Zakon o varstvu osebnih podatkov (ZVOP-1),[12] vendar pa je varstvo osebnih podatkov na delovnem mestu treba obravnavati tudi z vidika ureditve delovno pravnega področja. Zaradi varstva delavca, ki je v razmerju do delodajalca zagotovo šibkejša stranka, je zakonodajalec delovno pravno področje uredil predvsem z Zakonom o delovnih razmerjih (ZDR-1);[13] in Zakonom o evidencah na področju dela in socialne varnosti (ZEPDSV),[14] v katerih je opredelil, katere osebne podatke delavcev lahko delodajalec obdeluje. Glede na obstoječe določbe zakonodaja ne dopušča avtonomije strank v smislu, da bi delodajalec lahko od delavca zahteval ali obdeloval katere koli osebne podatke. Delodajalec mora v skladu s 46. členom ZDR-1 varovati in spoštovati delavčevo osebnost ter upoštevati in ščititi delavčevo zasebnost. V skladu z 48. členom

[12] Zakon o varstvu osebnih podatkov, Uradni list RS, št. 94/07 – uradno prečiščeno besedilo.
[13] Zakon o delovnih razmerjih, Ur. l. RS, št. 21/2013.
[14] Zakon o evidencah na področju dela in socialne varnosti, Ur. l. RS, št. 40/2006.

ZDR-1 lahko delodajalec načeloma zbira, obdeluje, uporablja in dostavlja tretjim osebam zgolj tiste osebne podatke delavcev, za katere je to določeno s tem ali drugim zakonom ali za katere je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem.

Uporabo službenih sredstev v delu, ki se nanaša na uporabo informacijsko-komunikacijske opreme v zasebne namene, vsaj v javnem sektorju še najbolj konkretno ureja Uredba o upravnem poslovanju (v nadaljevanju UUP).[15] Po UUP je uporaba informacijsko-komunikacijske opreme dovoljena v službene namene, izjemoma tudi v zasebne namene, vendar ta uporaba ne sme povzročati informacijskih tveganj in je dovoljena samo v zmernem obsegu, ki ne ovira ali ogroža normalnega delovnega procesa. 2. odstavek 70. člena UUP določa, da lahko predstojnik določi omejitve uporabe informacijsko-komunikacijske opreme. UUP tako postavlja samo pravila glede (dopustne) uporabe elektronske pošte in uporabe interneta, ne določa pa tudi možnosti vpogleda delodajalca v spletne strani, ki jih zaposleni obiskujejo, ali pa nadzora podatkov o poslani in prejeti elektronski pošti. Trenutna ureditev tako pušča veliko nedorečenosti, ki se – kot izhaja tudi iz prakse Informacijskega pooblaščenca – odraža tudi v kršitvah zakonodaje. V pripravi je Uredba o informacijski varnosti, ki naj bi povzela določene rešitve iz UUP ter dodatno razrešila vsaj nekatera od problematičnih vprašanj iz prakse – ravnanje s službenimi predali e-pošte po odhodu zaposlenega, hrambo podatkov o dostopu do interneta in uporabi elektronske pošte ter ravnanje s službeno opremo ob odhodu zaposlenega.

4. ISKANJE RAVNOVESJA

Glede na doslej predstavljeno obstaja očitna potreba po konkretni zakonski ureditvi problemskega področja. Trenutna zakonodaja na področju delovno-pravnih razmerij (ZDR-1, ZEPDSV ipd.) ter zakonodaja na področju varstva osebnih podatkov (ZVOP-1) namreč konkretno ne ureja tega področja, z izjemo dopustnosti uvedbe nekaterih oblik nadzora nad zaposlenimi, kot sta uvedba videonadzora in biometrijskih ukrepov.

Med pisanjem tega članka je bila dne 14. 4. 2016 v Evropskem parlamentu sprejeta Splošna uredba o varstvu osebnih podatkov (UREDBA (EU) 2016/679)

[15] Uredba o upravnem poslovanju, Uradni list RS, št. 20/2005 s spremembami in dopolnitvami.

Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov), ki na novo postavlja temelje varstva osebnih podatkov v EU. Z vidika obdelave osebnih podatkov zaposlenih je pomembno opozoriti na bolj izrecne omejitve veljavnosti privolitve v delovnih razmerjih – recital 42 tako med drugim določa, da »*Privolitev se ne bi smela šteti za prostovoljno, če posameznik, na katerega se nanašajo osebni podatki, nima možnosti dejanske ali prostovoljne izbire ali privolitve ne more zavrniti ali preklicati brez škode*.« Kakšen bo vpliv Splošne uredbe o varstvu podatkov na varstvo delavčeve informacijske zasebnosti, je v tem trenutku preuranjeno soditi – uredba bo stopila v uporabo v dveh letih od sprejema.

Informacijski pooblaščenec praktično od začetka svojega delovanja opozarja na odsotnost zakonodaje na področju varstva zasebnosti na delovnem mestu, ki bi v enem zakonu v celoti postavila temelje za ureditev vprašanja nadzora na delovnem mestu in uporabe elektronskih sredstev, kot so internet, elektronska pošta, mobilni telefoni ipd. Da bi se tovrstne dileme razrešile, je Informacijski pooblaščenec že leta 2009 pripravil osnutek Zakona o komunikacijski zasebnosti na delovnem mestu, katerega namen je določiti načela in pogoje za dopustnost posegov v informacijsko in komunikacijsko zasebnost ter dostojanstvo delavca pri uporabi sredstev za elektronsko komuniciranje na delovnem mestu, kot tudi pri uporabi službenega avtomobila oziroma obdelavi lokacijskih podatkov delavca. Informacijski pooblaščenec je osnutek omenjenega zakona že takrat posredoval Ministrstvu za delo, družino in socialne zadeve in Ministrstvu za pravosodje, kjer pa do nadaljnjih aktivnosti v zvezi s tem vse do sedaj še ni prišlo.[16]

V času odsotnosti izrecne pravne ureditve se delodajalcem priporoča sprejem internih aktov, s katerimi bi ob upoštevanju ustavnih in zakonskih pogojev ter sodne in nadzorne prakse transparentno in natančno uredili pogoje dopustne uporabe službenih sredstev v zasebne namene ter okoliščine in pogoje, v katerih lahko pride do nadzora takšne uporabe. Pri opredelitvi določil internih aktov je nujno potrebno opozoriti, da sama določila internih aktov ne smejo biti v neskladju z veljavno zakonodajo in ustavnimi določili, temveč mora biti vsak ukrep zakonit in ustavno dopusten. To pomeni, da tudi delodajalec, ki ne dopušča zasebne rabe (pri čemer je že tudi to lahko sporno), s sprejemanjem (in izvajanjem) določil svojih internih aktov ne sme kršiti ustavnih in zakonskih pravic posameznika do

[16] Informacijski pooblaščenec, 2010, str. 48.

informacijske in komunikacijske zasebnosti. Delodajalec ne sme biti zaveden v razmišljanju, da je s pripravo nekega pravilnika dobil blanketno dovoljenje, ki mu omogoča nadzor nad zaposlenimi. Tudi v takšnih primerih namreč ni dopustno spregledati načela sorazmernosti, po katerem morajo biti posegi v zasebnost posameznika utemeljeni in minimalni za dosego legitimnih, zakonitih in ustavno dopustnih ciljev.

Pri pripravi omenjenih internih aktov mora delodajalec upoštevati naslednja načela: popolnost, transparentnost, natančnost, nedvoumnost, zakonitost in ustavna dopustnost. Priporočljivo je, da so določbe kar se da natančne, nedvoumne in da zajamejo večino možnih situacij, kjer bi lahko prišlo do nezakonite obdelave osebnih podatkov oziroma posega v zasebnost zaposlenega (npr. ob prekinitvi delovnega razmerja, vračilu službene opreme, dopuščanju uporabe zasebnih naprav v službene namene)[17]. Kot je bilo pojasnjeno v opisu sodne prakse v EU, je delodajalec praviloma tisti, ki nosi posledice neustreznega informiranja zaposlenih. Določila internih aktov, na katera je naletel Informacijski pooblaščenec, kot so »Uporaba interneta s strani zaposlenih se lahko nadzira«, so v tem oziru v neskladju z navedenimi načeli. Nedopustna je tudi npr. naslednja določba: »V okviru rednih vzdrževalnih pregledov ali po naročilu odgovorne osebe informatik pregleduje dostope posameznikov do različnih spletnih naslovov in izdela poročilo pregleda dostopanja do svetovnega spleta.« Omenjena primera kažeta tudi na precejšnje nepoznavanje določb zakonodaje (predvsem ZVOP-1) na strani oseb, ki delajo v informatiki in ki so bile zavedene s funkcionalnostjo programov, ki jo omogočajo posamezne informacijsko-komunikacijske tehnologije in oprema.

Interni akt naj bi torej določil *pravila igre* – bolj kot bodo pravila igre jasna, manj bo prostora za dvoumnosti, in posledično manjše tveganje za posege v zasebnost, ki jo zaposleni upravičeno pričakuje (v razumni meji seveda, saj tudi njegove pravice niso absolutne) tudi na delovnem mestu. Priporočljivo je, da pri izdelavi omenjenih aktov sodelujejo sodelavci tako s pravnega kot z informacijskega področja, kajti le s sinergijo obeh ter medsebojno izmenjavo znanj lahko pridemo do pravno vzdržnih in hkrati tehnično izvedljivih internih aktov (Nataša Pirc Musar et al., 2008, str. 68).

[17] Podrobneje glej v Zasebnost delavcev in interesi delodajalcev – kje so meje. Uradni list Republike Slovenije, 2008.

5. ZAKLJUČEK

Zasebnost na delovnem mestu je predmet konfliktov med pravicami in interesi delodajalca, zaposlenih ter tretjih oseb. V trenutni situaciji, ko še ni sprejete izrecne pravne ureditve zadevnega področja, se priporoča sprejem internih aktov, s katerimi se lahko natančneje opredelijo okoliščine dopustne uporabe službenih sredstev v zasebne namene ter pogoji in okoliščine morebitnega nadzora, tako da ne bi prišlo do situacije, ko zaposleni ne bi vedeli, ali in pod kakšnimi pogoji so lahko nadzorovani. Nikakor pa ne gre pozabiti, da interni akti ne morejo postati bianco pooblastila za nadzor, ki ignorirajo ustavne in zakonske norme, temveč so lahko le mehanizem za doseganje transparentnosti do trenutka natančnejše zakonske ureditve, ki bo uravnovesila interes in pravice delodajalca in zaposlenih.

LITERATURA IN VIRI

- American Management Association/ePolicy Institute Research: 2001 Electronic Monitoring & Surveillance Survey. http://www.amanet.org/, 18. 5. 2005.
- American Management Association/ePolicy Institute Research: 2005 Electronic Monitoring & Surveillance Survey. http://www.amanet.org/, 9. 7. 2010.
- Cate, H. Fred: Privacy in the Information Age. Washington: Brookings Institution Press, 1997.
- Hunton&Willams: Germany Adopts Stricter Data Protection Law – Serious Impact on Business Compliance; http://www.hunton.com/files/tbl_s10News/FileUpload44/16482/germany_adopts_stricter_data_protection_law.pdf; 9. 7. 2010.
- Informacijski pooblaščenec: Letno poročilo Informacijskega pooblaščenca za leto 2009. Ljubljana: Informacijski pooblaščenec, 2010.
- Klemenčič, Goran: Internet in pravica do zasebnosti. V Bogataj, Maja (ur.), 2003. Internet in pravo, str. 101–141. Ljubljana: Pravna fakulteta, 2003.
- Kovačič, Matej: Nadzor in zasebnost v informacijski družbi. Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede, 2006.
- Pirc Musar, Nataša et. al: Zasebnost delavcev in interesi delodajalcev – kje so meje?. Ljubljana: Uradni list Republike Slovenije, 2008.
- UREDBA (EU) 2016/679 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).
- Evropsko sodišče za človekove pravice: sodba v primeru Bărbulescu proti Romuniji z dne 12. 1. 2016, št. 61496/08.
- Evropsko sodišče za človekove pravice: sodba v primeru Copland proti Združenemu kraljestvu z dne 3. 4. 2007, št. 62617/00.
- Evropsko sodišče za človekove pravice: sodba v primeru Halford proti Združenemu kraljestvu z dne 25. 6. 1997, št. 20605/92.

- Evropsko sodišče za človekove pravice: sodba v primeru Köpke proti Nemčiji z dne 5. 10. 2010, št. 420/07.
- Kasacijsko sodišče Francije: sodba v primeru Bruno B proti Giraud et Migot, 2009, št. 07-44264.
- Kasacijsko sodišče Francije: sodba v primeru M. X. proti Young & Rubicam France, 2013, št. 12-12.138.
- Kasacijsko sodišče Francije: sodba v primeru Societe Nikon France, SA proti Onof, 2001, št. 99–42.942.

PROTECTION OF WORKERS' INFORMATION PRIVACY

Andrej Tomšič*

SUMMARY

A common workplace in the information society is intrinsically connected with the intensive use of information and communication technologies and ubiquitous computing. The use of e-mail, internet and smartphones that enable greater accessibility of business applications, better mobility and availability of workforce benefits their productivity. The same information and communication technologies on the other hand enable collection and processing of personal data of employees – whom they call, which websites they visit, where they are, what and how much they are printing. It would be disproportionate to expect that employees never use their professional equipment also for private purposes to some extent, even vice versa – there are more cases where employees bring their own devices and use them for work related purposes. Processing of data about the use of information and communication technologies entails a conflict of interests between the employer and the employees, as well as third persons. In contrast to US, where the rights of the employer prevail, EU has decided to seek balance between different interests. In an area that is obviously under regulated, some directions may be sought in court cases of European Court of Human rights, national jurisprudence and practice of supervisory bodies. Substantial differences in these cases show that balancing the rights is a complex task which often depends on particular circumstances in each case. Assessing the reasonable expectation of privacy has become a key test and in this respect the role of internal regulation of organisations is paramount. Employers should be very precise and transparent towards their employees about their acceptable use polices and circumstances under which their use of professional equipment may be subject to monitoring. In any case one should bear in mind that technological

* Andrej Tomšič, Msc., Deputy Information Commissioner, Information Commissioner of the Republic of Slovenia
andrej.tomsic@ip-rs.si

(surveillance) solutions are not adequate if the source of the problem is in poor management and human resources, nor should they forbid something that is in its essence very human.