

Zasebnost in nadzor pri uporabi službenih sredstev

Andrej Tomšič*

UDK: 349.2:342.738:347

Povzetek: V prispevku je obravnavana problematika zasebnosti in nadzora na delovnem mestu z vidika uporabe službenih sredstev. Predstavljen bo konflikt med interesi delodajalcev, zaposlenih in tretjih oseb ter primeri sodne prakse, ki so pomembno vodilo za delodajalce ob odsotnosti jasne zakonske ureditve. Predstavljena bo ureditev za državne organe ter priporočila delodajalcem, kako vprašanja dopustne rabe službenih sredstev in nadzora nad njimi ustrezno urediti v internih aktih.

Ključne besede: zasebnost, varstvo osebnih podatkov, nadzor službenih sredstev, zasebnost na delovnem mestu, politike dopustne rabe službenih sredstev

Workplace Privacy and Surveillance

Abstract: The article deals with the issues of workplace privacy and surveillance when using workplace equipment and services. It depicts the conflict of interest between employers, employees and third parties and provides examples of court cases as important guidance for employers in the absence of normative rules in legislation. The existing rules for public administration are shown and recommendations are provided to employers how to adequately address the issues of workplace privacy and surveillance in their internal policies.

Key words: privacy, personal data protection, workplace surveillance, workplace privacy, acceptable use policies

* Andrej Tomšič, magister poslovnih ved, Informacijski pooblaščenec RS
Andrej.tomsic@ip-rs.si
Andrej Tomšič, Msc., Information Commissioner of the Republic of Slovenia.

1. O ZASEBNOSTI NA DELOVNEM MESTU

Vprašanje nadzora elektronskih sredstev, ki jih uporabljajo zaposleni in so v lasti delodajalca, zaznamuje konfliktnost interesov: delodajalca, delavcev in tretjih oseb. Delodajalci pogosto zagovarjajo stališče, da imajo vso pravico do nadzora nad informacijsko-komunikacijsko in drugo opremo, kot so osebni računalniki, mobilni telefoni, službena vozila, tiskalniki, multi-funkcijske naprave in tako naprej, saj da gre za opremo, ki je last delodajalca in ki je (zgolj) dana v uporabo zaposlenim. Ne nazadnje ima nad temi sredstvi lastninsko pravico, sredstva pa so bila dana zaposlenim v uporabo, da v imenu in za račun delodajalca opravljajo naloge in dela, ki so jim bila določena. Delodajalci prav tako računajo na to, da imajo pravico do nadzora nad tem, ali zaposleni službena sredstva uporabljajo ali celo zlorabljajo za zasebne namene, za kršitev internih aktov in pravilnikov, za pridobitniško dejavnost ali celo za storitev kaznivih dejanj. Službena sredstva so bila dana zaposlenim zato, da dosegajo cilje, ki jih zasleduje delodajalec in so last delodajalca, zato naj zaposleni ne bi imel pravice do zasebnosti pri uporabi službenih sredstev. Takšno stališče, ki ne upošteva pravic in interesov drugih, je razlog, da je na Informacijskega pooblaščenca vloženo veliko prijav na temo nadzora zaposlenih in tudi na splošno so vprašanja varstva osebnih podatkov v okviru delovno-pravnih razmerij med najbolj obsežnimi temami, s katerimi se ukvarja Informacijski pooblaščenec.

Delodajalci, ki ignorirajo pravice zaposlenih in tretjih oseb, pa lahko kaj kmalu prekoračijo meje dopustnega in zakonitega pri nadzoru uporabe interneta, elektronske pošte, gibanja zaposlenih, uporabe videonadzora in biometrije. Nadzor s strani delodajalcev dodatno spodbujajo zmogljivosti tehnologije in dostopnost rešitev za nadzor zaposlenih, ki pa večinoma izvirajo iz ZDA, kjer je nadzor delodajalca nad zaposlenimi glede uporabe službenih sredstev pogosto povsem dopusten, na kar nakazuje tudi tamkajšnja sodna praksa¹.

S tehničnega vidika je mogoče nadzorovati skoraj vse pojavne oblike informacijsko-komunikacijske tehnologije (IKT), na delovnem mestu pa so najpogostejše:

- nadzor nad uporabo službene IKT opreme (računalniki, telefoni, mrežni diski, tiskalniki ipd.),

¹ Glej npr. McLaren proti Microsoft I. '99. Podjetje je pregledalo šifrirano elektronsko pošto zaposlenega, shranjeno v računalniku v mapi "Osebni imenik"; zaposleni je zato sprožil sodni spor. Sodišče je v razsodbi dalo prav delodajalcu, saj naj bi interes delodajalca, da prepreči pošiljanje neprimerne elektronske pošte, bil nad pravico zaposlenega do zasebnosti.

- nadzor nad uporabo interneta (angl. cyberslacking),
- nadzor nad uporabo e-pošte,
- nadzor nad prihodi in odhodi z delovnega mesta (evidenčne kartice, biometrija ipd.),
- splošni videonadzor nad delom in gibanjem delavca,
- nadzor nad gibanjem delavca pri uporabi službenih vozil (npr. GPS sistemi),
- nadzor nad lokacijo oziroma gibanjem delavca znotraj službenih prostorov.

Delodajalec se lahko glede uporabe službenih sredstev hitro znajde v dilemi. Ali bo dovoljeval uporabo službenih sredstev zgolj v službene namene ali pa bo pod nekimi pogoji dopuščal uporabo tudi v zasebne namene? Omenjena odločitev je bistvena in mora biti v izogib težavam in dvomnostim že takoj na začetku jasno in natančno navedena v ustreznih internih aktih (pravilnikih, politikah ipd.). Transparentnost do zaposlenih je tudi eno ključnih priporočil v Priporočilu o varstvu osebnih podatkov v zvezi z zaposlovanjem Sveta ministrov EU iz leta 2015², v katerem ob odnosnosti podrobnejše zakonske ureditve še vedno najdemo nekaj najbolj konkretnih priporočil glede urejanja vprašanja nadzora in zasebnosti pri uporabi službenih sredstev.

Kot smo omenili na začetku, gre pri vprašanju nadzora službenih sredstev za konflikt med različnimi strankami in interesi. Na drugi stran so namreč zaposleni, ki smo še vedno predvsem ljudje in ki tudi takrat, ko prestopimo prag delodajalca, ne postanemo roboti, ki se v delovnem okolju odpovemo svojim temeljnim človekovim pravicam. Gre za pravice, ki jih zagotavlja že Ustava RS, konkretizira pa zakonodaja, čeravno je na tem področju še precej pomanjkljiva oziroma zadevne problematike ne ureja posebej natančno, ter sodna praksa, zlasti Evropskega sodišča za človekove pravice. Zakon o delovnih razmerjih (ZDR-1)³ je namreč glede pravic zaposlenih precej jasen. V Sloveniji noben zakon izrecno ne opredeljuje pravice delodajalca do posega v zasebnost zaposlenega, temveč kvečjemu obratno. 48. člen ZDR-1 določa, da mora

² Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies). Dostopno na: <https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282015%295&Language=lanEnglish&Ver=original&Site=CM&BackColorIntern et=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864>

³ 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, 81/19, 203/20 – ZIUPOPĐVE, 119/21 – ZČmIS-A, 202/21 – odl. US, 15/22, 54/22 – ZUPŠ-1 in 114/23.

delodajalec spoštovati in varovati delavčevo osebnost ter upoštevati in ščititi delavčevo zasebnost. Zakon še določa, da se lahko v delovnih razmerjih obdelujejo samo tisti osebni podatki, ki so nujni za uresničevanje pravic in obveznosti v delovnem razmerju. Sem verjetno ne spadajo podatki o tem, katero spletno stran smo obiskali, koliko časa smo preživeli na družabnih omrežjih in ali smo kdaj poklicali domov s službenega telefona. Sodna praksa Evropskega sodišča za človekove pravice je jasno pokazala, da zaposleni upravičeno pričakuje razumno mero pričakovane zasebnosti (tudi) na delovnem mestu in da človekove pravice ne izgubijo veljave s tem, ko prečkamo prag delodajalca. Tega seveda ne gre razumeti v smislu, da si lahko zaposleni na delovnem mestu privoščijo popolno svobodo in da lahko svojo pravico do zasebnosti izkoriščajo do take mere, da na drugi strani delodajalec nima nobene pravice, da bi jih nadziral. Gre predvsem za to, da je treba razumeti, da gre za tehtanje različnih pravic, od katerih nobena ni absolutna – ne pravica delodajalca do nadzora lastnine ne pravica zaposlenega do zasebnosti.

Kot da stanje ne bi bilo dovolj komplicirano z dvema različnima interesnima skupinama, pa se vprašanje nadzora na delovnem mestu dodatno zakomplicira s pomislekom na tretjo interesno stranko. Gre za tretje osebe, s katerimi zaposleni komunicirajo v službenem času. Zunanji sodelavci, poslovni partnerji, dobavitelji, kupci, prijatelji in družinski člani – z vsemi temi namreč zaposleni po naravi stvari komunicirajo v delovnem času. Problem je seveda v tem, da tretje osebe precej težje (ali sploh?) obvestimo o tem, da je lahko njihova komunikacija z zaposlenimi nadzorovana s strani delodajalca. Delodajalec namreč nima pravice nadzirati tretje osebe, ki je zaposlenemu poslala določeno elektronsko pošto, ga poklicala na službeni telefon in podobno.

2. NORMATIVNA UREDITEV

Uravnoteženje pravic delodajalca in zaposlenih na tem področju bi lahko uredil poseben zakon o zasebnosti in nadzoru na delovnem mestu – predlogi so bili že podani⁴, vendar pa za sprejem zakona ni bilo dovolj podpore. Še največ je z vidika normativne ureditve prinesla Uredba o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18, 131/20 in 49/23 – ZInIV-B; UIV), ki vsaj za

⁴ Osnutek takega zakona je že leta 2008 pripravil Informacijski pooblaščenec.

državno upravo vsebuje določene ureditve zadevne problematike. 39. člen UIV člen opredeljuje dopustno uporabo sistema elektronske pošte in določa, da je sistem elektronske pošte organa namenjen za službeno uporabo, vendar pa je uporaba za druge namene izjemoma dopustna, če ne ogroža varnosti informacijskega sistema organa, ne ovira službene uporabe sistema elektronske pošte in ne zmanjšuje učinkovitosti dela drugih uslužbencev organa. Uslužbenci organa morajo uporabljati sistem elektronske pošte tako, da pri tretjih osebah, ki so prejemniki elektronskih sporočil, ne nastane dvom, ali gre za službeno sporočilo ali zasebno sporočilo, ki je samo poslano s službenega elektronskega naslova. Za zagotovitev varnosti in nemotenega delovanja upravljavec sistema elektronske pošte ali predstojnik organa na podlagi ocene tveganja lahko med drugim omeji največjo velikost elektronskih sporočil, pošiljanje nekaterih vrst priponk. Peti odstavek 39. člena izrecno določa, da elektronske pošte ni dovoljeno samodejno preusmerjati na druge naslove, takšna pa je tudi inšpekcijska in (sodno potrjena) nadzorna praksa Informacijskega pooblaščenca⁵. Podobne ureditve za zasebni sektor ni, zato se delodajalci lahko hitro znajdejo pred dilemami, ali in do katere meje je dopusten nadzor zaposlenih pri uporabi službenih sredstev.

Na podoben način je v UIV urejena uporaba interneta – prvi odstavek 40. člen UIV določa, da uslužbenci organa uporabljajo internet za službene namene. Uslužbenci organa lahko internet izjemoma uporabljajo tudi za zasebne namene, vendar ta uporaba ne sme povzročati tveganj informacijske varnosti in je dovoljena samo v zmernem obsegu, ki ne ovira ali ogroža normalnega delovnega procesa. Drugi odstavek 40. člena UIV določa, da uporaba interneta vsebinsko ni omejena, omogoča pa tehnično omejevanje dostopa do določenih spletnih mest in storitev na podlagi ocene tveganja in drugih okoliščin. Omeji se lahko dostop do spletnih mest in storitev, ki lahko vsebujejo škodljivo programsko kodo ali kako drugače ogrožajo informacijska premoženja in sisteme državne uprave, ki lahko negativno vplivajo na razpoložljivost in odzivnost informacijskih in komunikacijskih sistemov, ki kršijo avtorske pravice (npr. strani s piratskimi vsebinami), katerih vsebina lahko neposredno ali posredno ogrozi državno varnost in državljanke, katerih vsebina bi bila lahko žaljiva za posamezne osebe ali skupine, če bi tak dostop lahko škodil ugledu organa ali če bi tak dostop lahko povzročil odškodninsko odgovornost organa⁶.

⁵ Dostopno na: <https://www.ip-rs.si/varstvo-osebnih-podatkov/praksa-ip>.

⁶ Takšne omejitve so tudi implementirani v omrežju HKOM (Hitro komunikacijsko omrežje državnih organov), ki ga uporabljajo državni organi in nekateri drugi organi javne uprave.

Za utrditev razumevanja o pravici zaposlenih do razumne mere zasebnosti na delovnem mestu si lahko vsakdo postavi naslednja vprašanja. Kdo ni nikoli poklical domov s službenega telefona? Kdo ni nikoli v službi poslal elektronske pošte, ki ni bila službene narave? In kdo si ni nikoli v službi ogledal spletne strani (na službenem računalniku in v delovnem času!), ki ni imela nobene zveze z delom? Hitro lahko pridemo do zaključka, da take osebe tudi v krogu vodstva pri delodajalcu ni, posledično pa si moramo priznati, da smo vsi krvavi pod kožo in da težko ignoriramo, da ne obstaja pričakovana raven zasebnosti na delovnem mestu.

Za delodajalce, ki skušajo uravnotežiti lastne pravice in pravice zaposlenih pri uporabi službenih sredstev je bistveno, da s vnaprej opredelijo »pravila igre« – kaj je dovoljeno v delovnem okolju in kaj ne ter v kakšnih okoliščinah in pod kakšnimi pogoji je določena aktivnost zaposlenega nadzorovana. Pri tem je priporočljivo, da delodajalec upošteva naslednja načela: popolnost, transparentnost, natančnost, nedvoumnost, zakonitost, ustavna dopustnost.

Z načelom popolnosti je mišljeno, da mora opraviti presojo, kdaj vse bo pri uporabi službenih sredstev hote ali nehote zbral osebne podatke zaposlenih. Tipični primeri, ki so zelo pogosti, če ne celo neizogibni v večini delovnih okolij, so vračilo službene opreme (npr. računalnikov in mobilnih telefonov) ob odhodu zaposlenega, uporaba mrežnih tiskalnikov in multi-funkcijskih naprav ter uporaba kartic za odpiranje vrat⁷. Vračilo službene opreme je primer situacije, ki se prav gotovo pojavlja v vsakem delovnem okolju, verjetno pa je mnogo delodajalcev, ki tega postopka nima opredeljenega v internih aktih, posledično pa se pojavijo številna vprašanja. Ali ima zaposleni pravico do izbrisa zasebnih podatkov s službenega računalnika ali telefona, kdaj in kako lahko to izvede, ali bo dejansko fizično resnično uspel izbrisati podatke zasebne narave (o obiskanih spletnih straneh, piškotke, zasebne dokumente, fotografije ipd.), ali prav ravna delodajalec, ki zaposlenemu ne da te možnosti in kako pravilno ravnati, če se delodajalec boji, da bo zaposleni, s katerimi prekinja delovno razmerje, ob takšni ponujeni priložnosti le še nadaljeval s povzročanjem škode delodajalcu? Delodajalec je sicer lastnik službenega sredstva, ni pa avtomatsko lastnik tudi vseh podatkov, ki se nahajajo na službenem sredstvu. Pravilno bo ravnal delodajalec, ki bo zaposlenemu ponudil možnost, da v razumnem roku pred

⁷ S tem mislimo na kartice, ki omogočajo odpiranje vrat v notranjih prostorih delodajalca in ne uporabo kartic za evidentiranje delovnega časa.

odhodom s službenih sredstev izbriše (oziroma si prekopira) podatke zasebne narave, nato pa z delodajalcem podpiše primopredajni zapisnik, s katerim potrdi, da mu je bila ta možnost dana, da jo je uporabil in da se na službenem sredstvu, ki ga vrača ne nahajajo več podatki oz. informacije zasebne narave, temveč le še podatki službene narave. Delodajalec lahko takšno delovno sredstvo preda v uporabo drugemu zaposlenemu, ga formatira, odpiše oziroma z njim prosto razpolaga. V primeru sporov oz. ko zaposleni ne želi uporabiti te možnosti je pravilno postopanje delodajalca, da komisijsko in zapisniško pregleda službeno delovno sredstvo in poskusi ločiti podatke službene narave od podatkov zasebne narave.

Načelo transparentnosti, natančnosti in nedvoumnosti gre razumeti v smeri, da mora biti ureditev v internih aktih do zaposlenega jasna, natančna in razumljiva, da se bo zaposleni zavedal, kaj, kdaj in v kakšnih okoliščinah je predmet nadzora ter kakšna je dopustna uporaba službenih sredstev. Določbe internih aktov, kot so »*Uporaba interneta s strani zaposlenih se lahko nadzira.*«, ali pa »*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.*« ne izpolnjujejo kriterijev jasnosti in natančnosti, saj zaposleni iz njih ne morejo razbrati obsega, intenzivnosti, okoliščin ter posledic tovrstnega nadzora.

Z načelom zakonitosti in ustavne dopustnosti pa je predvsem mišljeno, da se morajo delodajalci zavedati, da ureditev v internih aktih ne sme presegati meje zakonitega in ustavno dopustnega in da ne more predstavljati *bianco* norme za delodajalčev nadzor.

Kot smo že omenili gre pri zasebnosti in nadzoru na delovnem mestu za področje, ki je pravno še vedno precej neurejeno. Delno lahko iščemo iztočnice za ureditev v Ustavi RS. Tako 37. člen ustave varuje komunikacijsko zasebnost posameznika, ki velja tudi na delovnem mestu, komunikacijsko zasebnost pa je mogoče prekršiti le ob zelo strogih pogojih, ki - ob strogem tolmačenju 37. člena Ustave RS - delodajalcu sploh ne omogočajo posega v komunikacijsko zasebnost zaposlenega (npr. vpogled v korespondenco prek elektronske pošte na službenem računalniku). Poseg bi namreč terjal kumulativno izpolnjevanje pogojev: da je podana podlaga v zakonu, da je bila pridobljena odredba sodišča, da je poseg omejen na določen čas in da je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. V praksi pa je že videti nekaj odstopanj od takšne stroge interpretacije drugega

odstavka 37. člena Ustave RS - v pravnih postopkih so že bile izdane odredbe za preiskavo nosilcev podatkov (v okviru predpravnega zavarovanja dokazov), nekateri zakoni pa dovoljujejo pregled elektronske korespondence, čeprav ne gre za postopke s področja pregona kaznivih dejanj ali za varnost države (npr. Zakon o preprečevanju omejevanja konkurence (ZPOmK-2⁸).

3. SODNA PRAKSA

Izjemnega pomena je sodna praksa sodišč, po kateri se zgledujejo tudi druga sodišča in predlagatelji zakonodaje. Eden prvih in najbolj znanih primerov sodne prakse na temo zasebnosti in nadzora na delovnem mestu je sodba Evropskega sodišča za človekove pravice v primeru *Halford proti Veliki Britaniji* iz leta 1997 v zvezi s kršitvijo 8. člena Evropske konvencije o človekovih pravicah⁹. Policistka Halford je v tem primeru tožila delodajalca, ker naj bi jo ta odpustil zaradi spolne diskriminacije, delodajalec (policija) pa je v svojo obrambo uporabila podatke o klicih, ki jih je policistka opravila s službenega telefona. V tem primeru je sodišče ugotovilo, da je imela policistka pri uporabi službenega telefona pravico do pričakovanja zasebnosti, saj vnaprej ni bila obveščena, da so lahko njeni klici nadzorovani. Evropsko sodišče za človekove pravice je torej jasno zapisalo, da ima posameznik pravico do varovanja zasebnosti tudi na delovnem mestu in tudi pri uporabi službenih komunikacijskih sredstev. Pri uporabi telefona se je celo izoblikovalo stališče, da pravnega varstva ne zasluži zgolj sama vsebina pogovora, ampak tudi vsi podatki, povezani s telefonsko komunikacijo, kot so spremljanje klicanih števil z nekega telefona, čas klica in trajanje pogovora.

Še dlje kot v primeru *Halford* je šlo Kasacijsko sodišče Francije v primeru *Societe Nikon France, SA, proti Onof* iz leta 2001, ko je zapisalo: »Delodajalec, ki bere sporočila, ki jih zaposleni pošilja ali sprejema prek službenega računalnika, krši temeljne pravice delavca, kot jih določa 8. člen Evropske konvencije o človekovih pravicah ... To velja ne glede na to, ali je bil delavec vnaprej seznanjen, da službenega računalnika ne sme uporabljati v neslužbene namene ... Podjetje ali druge ustanove ne smejo biti mesta, na katerih

⁸ Uradni list RS, št. 36/08, 40/09, 26/11, 87/11, 57/12, 39/13 – odl. US, 63/13 – ZS-K, 33/14, 76/15, 23/17 in 130/22. Glej npr. peti odstavek 29. člena ZPOmK-2.

⁹ Evropsko sodišče za človekove pravice: *HALFORD v. THE UNITED KINGDOM* (20605/92). Dostopno na: [https://hudoc.echr.coe.int/tur#{%22itemid%22:\[%22001-58039%22\]}](https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-58039%22]})

bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, v katerih temeljne človekove pravice nimajo veljave ... Menimo, da je splošna popolna prepoved uporabe e-pošte v neslužbene namene nerealna in krši pravno načelo sorazmernosti.» Če pomislimo na zgoraj zastavljena vprašanja, ali smo kdaj »zlorabili« službeno opremo v zasebne namene, se verjetno lahko strinjamo, da je omenjeno sodišče do navedenih zaključkov prišlo iz resničnih, življenjskih ravnanj vsakega posameznika.

Vendar pa sodna praksa včasih »zaniha« tudi v prid delodajalca, kot sta sodbi francoskega Kasacijskega sodišča Francije v primeru *Bruno B v. Giraud et Migot*¹⁰ ter v primeru *Monsieur X*¹¹, kjer je šlo za pričakovanje zasebnosti v primeru neoznačenih zasebnih datotek. Sodišče je stopilo na stran delodajalcev z interpretacijo, da ima tudi zaposleni nekaj dolžnosti, če naj se vzpostavi raven pričakovane zasebnosti in sicer naj bi vsaj nedvoumno označil, katere datoteke ali mape vsebujejo njegove zasebne podatke in ne službenih in na katerih pričakuje določeno mejo zasebnosti. Delodajalec namreč v nasprotnem primeru ne more vedeti, kje je tista meja, ki je ne bi smel prekoračiti pri nadzoru uporabe službenih sredstev, saj ne more vedeti, za katere podatke zaposleni želi, da so in ostanejo zasebne. Sodišče je zapisalo, da ima delodajalec, razen če dokumenti na službenem delovnem sredstvu niso jasno označeni kot »zasebni«, legitimno pravico predvidevati, da gre za dokumente službene narave in da so kot taki na voljo delodajalcu, tudi v primeru delavčeve odsotnosti.

Sodna praksa v Sloveniji je na tem področju dokaj skopa, z nekaterimi primeri pa se je ukvarjal Informacijski pooblaščenec. Informacijski pooblaščenec je v nekaj primerih odkril, da je s strani delodajalca prišlo do nezakonite obdelave osebnih podatkov, zato so bili zoper delodajalca in njegove odgovorne osebe uvedeni postopki o prekršku. V enem od takih primerov so zaposleni v službi za informatiko spremljali dostope zaposlenih do spletnih strani in o tem obveščali nadrejene. Delodajalec bi za obdelavo teh podatkov, ki so nedvomno osebni podatki, čeprav »nastajajo« na delovnem mestu, moral razpolagati s pravno podlago, bodisi v zakonu bodisi v osebni privolitvi posameznika. Ker delodajalec ni imel podlage v zakonu, zaposleni pa o tem, da uporaba interneta v zasebne namene ni dovoljena ter da se beleži njihova uporaba spletnih strani, niso bili obveščeni, je delodajalec nezakonito obdeloval osebne podatke.

¹⁰ Bruno B v. Giraud et Migot Cour de Cassation [Cass.], soc., Paris, 15 Dec. 2009, No. 07-44264.

¹¹ Monsieur X v. Young & Rubicam France, Cour de Cassation [Cass.], soc., 19 June 2013, No. 12-12138.

Informacijski pooblaščenec se je prav tako ukvarjal z več primeri nezakonitih ravnanj na področju videonadzora ter sumov, da nadrejeni zaposlenim prebirajo elektronsko pošto. Pri tem je treba poudariti, da gre pri takih ravnanjih lahko tudi za storitev katerega od kaznivih dejanj (npr. kršitev tajnosti občil), za katere pa Informacijski pooblaščenec ni pristojen, temveč se s temi primeri ukvarja policija oziroma tožilstvo. Posebej zanimiva je nadzorna in sodna praksa glede nadzora podatkov o uporabi službenih telefonov. Informacijski pooblaščenec je odločal glede nadzora službenih klicev na ljubljanskem okrožnem sodišču¹² ter na Ministrstvu za zunanje zadeve,¹³ in upravno sodišče je pritrdilo stališču Informacijskega pooblaščenca, da vodstvo delodajalca (ob povodu domnevnega nedopustnega razkrivanja informacij medijem) nima pravne podlage za nadzor nad podatki o tem, kdo je kdaj klical koga s službenega telefona.¹⁴

Na pomembnost ustrezne obveščenosti zaposlenega o nadzoru uporabe službenih sredstev - pri čemer pa se postavlja vprašanje dopustnosti in primernosti ter dejanske prostovoljnosti njihovega soglasja v spremljanje elektronskega prometa - nakazuje tudi sodna praksa Višjega sodišča v Ljubljani,¹⁵ ki je v zadevi *VSL0023190* zapisalo, da ker je bil obdolženec opozorjen na možnost, da bo delodajalec spremljal promet njegove elektronske pošiljke, s čimer je soglašal, pri uporabi službene elektronske pošte ni mogel pričakovati popolne zasebnosti pri komunikaciji. Zato vsebina službene elektronske pošte, čeprav jo je sodišču predložil delodajalec, ne pomeni nedovoljenega dokaza, na katerega se sodba ne bi smela opirati. Podobno se je Vrhovno sodišče v kazenski zadevi *VSL I Kp 1344/2007*¹⁶ postavilo na stališče, da obsojenka, ki je bila opozorjena na možnost, da bo delodajalec spremljal promet z elektronsko pošto in je s tem soglašala, pri uporabi službene elektronske pošte ni mogla

¹² Medijsko poročanje: <https://www.24ur.com/novice/slovenija/baragi-globa-zaradi-preverjanja-telefonskih-klicev.html>

¹³ T.i. afera washingtonska depeša (<https://www.dnevnik.si/321759>).

¹⁴ Zanimiva je tudi sodba Upravnega sodišča sodba U 702/99 iz leta 2000, ko je delodajalec iskal žvižgače iskali žvižgače (ti so nato tožili delodajalca), kjer je sodišče potrdilo horizontalno uporabnost 37. člena Ustave RS (»Varstvo zasebnosti, zagotovljeno v 37. členu Ustave, se uporabi tudi za področje nadzora nad rabo telefonskih aparatov, dodeljenih posameznikom sicer za službeno uporabo.«).

¹⁵ VSL0023190, 14.01.2015, [http://sodnapraksa.si/?q=slu%C5%BEbena%20elektronska%20po%C5%A1ta&database\[SOVS\]=SOVS&database\[IESP\]=IESP&database\[VDSS\]=VDSS&database\[UPRS\]=UPRS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2012032113077803](http://sodnapraksa.si/?q=slu%C5%BEbena%20elektronska%20po%C5%A1ta&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2012032113077803)

¹⁶ [https://www.sodnapraksa.si/?q=*&database\[SOVS\]=SOVS&database\[IESP\]=IESP&database\[VDSS\]=VDSS&database\[UPRS\]=UPRS&_submit=i%C5%A1%C4%8Di&id=22610](https://www.sodnapraksa.si/?q=*&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&id=22610)

pričakovati popolne zasebnosti in zato izpis o prometu elektronske pošte tudi ne predstavlja nedovoljenega dokaza.

Med recentnimi sodbami je morda še največ medijskega poročanja doživela sodba Evropskega sodišča za človekove pravice v primeru *Barbulescu proti Romuniji*, 2016 (št. 61496/08). Šlo je za nadzor uporabe spletnega klepetalnika, ki je bil namenjen za odgovore strankam. Zaposleni je bil jasno vnaprej obveščen o prepovedi uporabe računa za zasebne namene, a se je izkazalo, da je večinoma bil nedosegljiv za stranke, saj je klepetalnik uporabljal za pogovore z zaročenko in bratom. Evropsko sodišče za človekove pravice je zapisalo, da je bil nadzor uporabe internetne storitve in posledična odpustitev zaposlenega upravičena. Poslovni časniki so se takrat razpisali o koncu zasebnosti na delovnem mestu, a je treba opozoriti, da je šlo za konkreten primer in specifične konkretne okoliščine, ki jih ni primerno posploševati, ker je zaposleni dal pisno izjavo, da je klepetalnik uporabljal samo v službene namene - nadzor delodajalca je bil zato pričakovan in razumen, ker so določbe Ustave RS glede varstva komunikacijske zasebnosti strožje in ker je bilo kar nekaj nejasnosti glede samega primera (predvsem kakšen je bil povod za nadzor delodajalca). Na koncu je sodba „padla“ pred Velikim Senatom ESČP, ki je zapisalo, da zaposleni ni bil informiran o obsegu in naravi nadzorovalnih aktivnosti in možnosti, da ima delodajalec dostop do vse vsebine njegove komunikacije ter da nacionalna sodišča niso posvetila dovolj pozornosti obsegu nadzora, stopnji posega in sami upravičenosti nadzora nad komunikacijo, saj da konkreten razlog nadzora ni bil določen niti niso bile preučene možnosti milejšega posega v pravice posameznika.

4. KJE JE TOREJ MEJA?

Do sprejema zakonodaje, ki bi natančneje opredelila pravila, se priporoča oblikovanje internih aktov (navodil, pravilnikov ipd.), kjer je treba čim bolj natančno postaviti pravila in poskušati razmejiti službeno rabo elektronskih sredstev od (dopustne) zasebne rabe ter pri tem slediti nadzorni in sodni praksi. Če delodajalec dopušča (zmerno) rabo službenih sredstev tudi v zasebne namene – in veliko jih to zaradi produktivnosti in ugodnega delovnega okolja dopušča – je pravilno, da tudi o tem jasno seznani zaposlene. Gre za iskanje razumne mere zasebnosti na delovnem mestu, ki ne vodi v poslabšanje učinkovitosti, ne

povzroča previsokih stroškov ali izgub, po drugi strani pa lahko deluje stimulatивно na zaposlene, na kakovost in učinkovitost dela, razvoj medsebojnih odnosov in pripadnosti organizaciji. Delodajalci pa bi se predvsem morali zavedati, da ni najbolj primerno reševati težav, ki so primarno organizacijske in upravljske narave s tehnološkimi ukrepi – ustrezno odrejanje delovnih nalog ter nadzor nad obsegom in kakovostjo opravljenega dela se izkaže bolj učinkovito in manj sporno kot nadzorovanje »ne-dela« s tehničnimi sredstvi.

LITERATURA IN VIRI

- Cour de Cassation [Cass.], soc., Paris Monsieur X v. Young & Rubicam France, 19 June 2013, No. 12-12138.
- Cour de Cassation [Cass.], soc., Paris: Bruno B v. Giraud et Migot, 15 Dec. 2009, No. 07-44264.
- Evropsko sodišče za človekove pravice: HALFORD v. THE UNITED KINGDOM (20605/92). Dostopno na: <https://hudoc.echr.coe.int/tur#%7B%22itemid%22%3A%22001-58039%22%7D>
- Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (1.4.2025, 1224th meeting of the Ministers' Deputies). Dostopno na: <https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282015%295&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864>
- Upravno sodišče: sodba U 702/99, 21.3. 2000. Dostopno na: [https://www.sodnapraksa.si/?q=id:60177&database\[SOVS\]=SOVS&database\[IESP\]=IESP&database\[VDSS\]=VDSS&database\[UPRS\]=UPRS&_submit=i%C5%A1%C4%8Di&id=60177](https://www.sodnapraksa.si/?q=id:60177&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&id=60177)
- Uredba o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18, 131/20 in 49/23 – ZInfV-B; UIV)
- Vrhovno sodišče: zadeva VSL I Kp 1344/2007, 11.12.2008. Dostopno na: [https://www.sodnapraksa.si/?q=*&database\[SOVS\]=SOVS&database\[IESP\]=IESP&database\[VDSS\]=VDSS&database\[UPRS\]=UPRS&_submit=i%C5%A1%C4%8Di&id=22610](https://www.sodnapraksa.si/?q=*&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&id=22610)
- Vrhovno sodišče: zadeva VSL0023190, 14.01.2015, [http://sodnapraksa.si/?q=slu%C5%BEbena%20elektronska%20po%C5%A1ta&database\[SOVS\]=SOVS&database\[IESP\]=IESP&database\[VDSS\]=VDSS&database\[UPRS\]=UPRS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2012032113077803](http://sodnapraksa.si/?q=slu%C5%BEbena%20elektronska%20po%C5%A1ta&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2012032113077803)
- Zakon o delovnih razmerjih ((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, 81/19, 203/20 – ZIUPOPDVE, 119/21 – ZČmIS-A, 202/21 – odl. US, 15/22, 54/22 – ZUPŠ-1 in 114/23; ZDR-1)
- Zakon o preprečevanju omejevanja konkurence (Uradni list RS, št. 36/08, 40/09, 26/11, 87/11, 57/12, 39/13 – odl. US, 63/13 – ZS-K, 33/14, 76/15, 23/17 in 130/22 – ZPOmK-2)

Workplace Privacy and Surveillance

Andrej Tomšič*

Summary

Given that the use of internet, email, telephones and other information and communication technologies at workplace inevitably entails processing of personal data, conflicts between involved parties, i.e., the employer, the employees and third persons are potentially and practically unavoidable. Employers tend to defend their stance that it is their equipment which was merely given to employees to perform tasks for the employer hence they have every right to conduct surveillance how and what for it is used, especially to ascertain whether it is used for private purposes or even illegal activities. Employers that ignore that individuals' human rights also exist in professional environments are likely to overstep the allowed boundaries in surveillance of internet, e-mail and other equipment and services usage by their employees.

The issues of workplace privacy and surveillance remain mostly unaddressed in terms of legislation therefore the employers need to refer to supervisory and court practice. The judgments of the European Court of Human Rights have clearly shown that the employees legitimately expect a certain degree of privacy also at their workplace and that human rights should not be diminished in working environments. It is important to understand that it is about weighing different rights and interests of which none is absolute – neither the right of the employer to control its own property nor the right of employees to privacy. Court cases show that also the employees have certain obligations in establishing this balance, for example by clearly marking which segments of information are of private nature where they consider their privacy needs to be respected.

In the absence of the issues being clearly legislated and balance determined, employers are advised to clearly set the rules of appropriate use of workplace equipment and services in their internal policies so the employees can understand what the boundaries are and what and under which circumstances they could be subjected to surveillance. In doing so, the employers should take into account the principles of comprehensiveness, transparency, clarity

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

and precision while staying within the boundaries of what is lawfully and constitutionally acceptable. The rules should be easy to understand and clear as the employees.

The article concludes with the recommendation that in workplace environments the management should not try to solve organizational and managerial issues with the introduction of technological surveillance tools, but rather by adequately controlling the amount and fulfillment of the tasks given to the employees. What should be surveilled is work and not lack thereof.