UDK: 342.738:004.056

Stručni rad

MERE ELEKTRONSKOG NADZORA ZAPOSLENIH I PRAVO NA PRIVATNOST NA RADNOM MESTU

Ivan Žarković[1]
Ministarstvo unutrašnjih poslova Republike Srbije

Sažetak: Savremeni razvoj tehnologije omogućio je primenu raznovrsnih sistema nadzora radnog okruženja. Mnogi poslodavci smatraju da je nadzor radnog okruženja ključna pretpostavka njegove bezbednosti, ali i produktivnosti zaposlenih. Nezavisno od toga o kojoj vrsti nadzora se radi, poslodavci moraju voditi računa da ne zloupotrebe nadzor i time naruše prava zaposlenih. Imajući u vidu aktuelne oblike elektronskog nadzora zaposlenih, ciljeve koji se nadzorom postižu, kao i rizike od potencijalnog kršenja prava zaposlenih, neizbežno je postaviti pitanje postojanja i efikasnosti mera zaštite ličnih podataka zaposlenih i njihove privatnosti na radnom mestu. Kao jedan od najčešćih vidova nadzora radnog prostora, video-nadzor privlači naročitu pažnju i praktičara i teoretičara. S obzirom na rečeno, kroz predstavljanje zakonskog osnova i okvira postavljanja i korišćenja sistema video-nadzora, u tekstu koji sledi biće analizirana neka od spornih pitanja koja se tim povodom postavljaju. Pored ovoga, ukazaće se i na pojedine presude Evropskog suda za ljudska prava u kojima se odlučivalo o pravu na privatnost zaposlenih.

Ključne reči: elektronski nadzor, video-nadzor, privatnost, poslodavac, zaposleni.

Uvod

Nadzor zaposlenih na radnom mestu nije pojava novijeg datuma, a naučno-tehnički razvoj omogućio je poslodavcima da, u cilju zaštite svojih interesa, uz postojeće, počnu da koriste i raznovrsne sofisticirane metode.

Instalacija i eksploatacija raznovrsnih sistema nadzora na radnom mestu omogućava efikasnije ostvarivanje različitih ciljeva, a među njima i prevenciju

1 Specijalista kriminalista, e-mail: ivan.zarkovic@mup.gov.rs.

vršenja prekršajnih ili krivičnih dela čiji su objekti napada imovina i druge vrednosti poslodavca i zaposlenih, odnosno njihovo efikasnije otkrivanje, rasvetljavanje i dokazivanje.

Iako za najveći broj subjekata neprimetne i naizgled neometajuće, ove tehnologije mogu da budu vrlo invazivne. Stoga se, s razlogom, sve češće postavljaju i pitanja pravnog osnova njihove primene, dozvoljenosti i granica zadiranja u ljudska prava zaposlenih (posebno prava na privatnost i njegovog ograničenja na radnom mestu), kao i ugrožavanja dostojanstva zaposlenih.

Rezultati studije koju je 2007. godine sprovela Američka asocijacija za menadžment (*American management association*, u daljem tekstu AMA) u saradnji sa institutom *ePolicy* pokazali su da 11% kompanija[2] koristi globalni sistem za praćenje putem satelita (u daljem tekstu – GPS)[3], da 52% koristi *smart cards* (pametne kartice) kao vid zaštite pristupa određenim zgradama ili centrima za obradu podataka.[4] Studija je takođe pokazala da 66% poslodavaca vrši nadzor nad internet sadržajima koje posećuju njihovi zaposleni (sa ciljem sprečavanja „nedozvoljenog" pretraživanja internetom), a da 65% kompanija koristi specijalizovane softvere kako bi blokirali pristup stranicama za koje smatraju da nisu u vezi sa obavljanjem posla[5].

Studija je pokazala da je više od jedne trećine (28%) kompanija otpustilo radnike zbog zloupotrebe *e-mail*-a[6], a kao razlozi su (pojedinačno ili zajedno sa drugim razlozima) navedeni: kršenje neke od politika kompanije (64%), neprikladan ili uvredljiv govor (62%), preterana lična upotreba (26%), kršenje pravila poverljivosti (22%) i nešto drugo (12%). [7]

Kada je reč o nadzoru interneta, 30% poslodavaca otpustilo je radnike zbog zloupotrebe ove mreže, a kao razlozi (pojedinačno ili zajedno sa drugim razlozima), navedeni su: gledanje, preuzimanje ili otpremanje neprikladnog/

2 Studijom su bili obuhvaćeni podaci prikupljeni u periodu 2001–2007. godine u 304 kompanije (27% kompanija zapošljavalo je 100 ili manje radnika, odnosno od 101 do 500 zaposlenih, po 12% kompanija zapošljavalo je od 501 do 1000 i od 1001 do 2500 radnika, 10% od 2501 do 5000 radnika, a više od 5001 zaposlenog zapošljavalo je 12% kompanija). Na pitanje koja delatnost najbolje opisuje sferu poslovanja njihove kompanije, 21% ispitanika je naveo da je to sfera biznisa / poslovnih usluga, njih 19% da je to proizvodnja, 12% da je u pitanju javna uprava, 7% da su u pitanju finansijske usluge, 4% da je reč o veleprodaji/maloprodaji, 2% da su u pitanju opšte usluge, a 35% ispitanika je navelo da su u pitanju ostale delatnosti. Preuzeto sa: http://www.epolicyinstitute.com/2007-survey-results (1. 7. 2015).

3 GPS predstavlja za sada zvanično jedini potpuno funkcionalan sistem za određivanje pozicije korisnika na bilo kojoj tački na planeti. Korišćenjem konstelacije od dvadeset i četiri satelita koji emituju specijalno kodirane radio signale, proračunava se tačna pozicija u koordinatnom sistemu geografske dužine, širine i nadmorske visine. Pored proračunavanja pozicije, moguće je dobiti i informaciju o brzini kretanja nosioca prijemnika.

4 *Smart card* (pametna kartica) plastična je kartica, veličine kreditne kartice, sa ugrađenim elektronskim kolom (mikročipom) koji sadrži kodirane podatke i koja se, između ostalog, može koristiti kako bi se pružio pristup zaštićenim oblastima ili sistemima. Identifikacioni dokument u vidu pametne kartice mora da sadrži sliku i podatke o imenu i prezimenu nosioca, potpis, datum isteka i identifikacioni broj.

5 U ovom segmentu evidentirano je povećanje od 27% u odnosu na 2001. godinu kada je istraživanje prvi put sprovedeno.

6 U izveštaju AMA navodi se da *e-mail* nadgleda 43% kompanija.

7 The Epolicy Institute, 2007 Electronic Monitoring & Surveillance Survey, dostupno na: http://www.epolicyinstitute.com/2007-survey-results (1. 7. 2015).

uvredljivog sadržaja (84%), kršenje bilo koje politike preduzeća (48%), preterana lična upotreba (34%) i nešto drugo (9%).[8]

U pogledu normativnog osnova, faktičkih razloga i opravdanosti uvođenja novih tehnologija nadzora u savremeno poslovanje, u teoriji i među praktičarima, prisutni su različiti, često i krajnje suprotstavljeni stavovi.

Važno je napomenuti da u zakonodavstvu Republike Srbije ne postoji zakon koji sveobuhvatno reguliše primenu nadzora na radnom mestu, kao i to da se zloupotrebom sistema nadzora mogu izvršiti različita krivična dela predviđena Krivičnim zakonikom Republike Srbije[9] (u daljem tekstu KZ): povreda tajnosti pisama i drugih pošiljki (čl. 142 KZ), neovlašćeno prisluškivanje i snimanje (čl. 143 KZ), neovlašćeno fotografisanje (čl. 144 KZ), neovlašćeno objavljivanje i prikazivanje tuđih spisa, portreta i snimaka (čl. 145 KZ) i neovlašćeno prikupljanje ličnih podataka (čl. 146 KZ).[10]

1. Elektronski nadzor zaposlenih

Ubrzani tehničko-tehnološki napredak u svim sferama, a samim tim i u sferi telekomunikacija i informatike, kao i potreba za što „bržim" imenovanjem novih sistema, predmeta i pojava, doveli su do sve većeg „pozajmljivanja" reči i fraza iz stranih jezika[11]. Engleski jezik danas se smatra međunarodnim jezikom u mnogim oblastima poslovanja, ekonomije, nauke, tehnologije. S obzirom na navedeno, većina novih tehnologija prvo dobija naziv na engleskom jeziku, a samim tim i nazive dobijaju i domeni primene savremenih uređaja i sistema[12].

Kada je reč o nadzoru zaposlenih, termini koji se koriste su *monitoring* i *surveillance*, odnosno nadgledanje i nadzor. Navedeni termini se uglavnom koriste kao sinonimi. Pod elektronskim nadzorom zaposlenih podrazumeva se računarsko prikupljanje, čuvanje, analiziranje i izveštavanje o informacijama vezanim za aktivnosti zaposlenih.[13] U normativnim aktima Sjedinjenih Američkih Država, u državi Konektikat termin „elektronski nadzor zaposlenih" podrazumeva prikupljanje podataka na objektima poslodavca koji se tiču aktivnosti ili komunikacija zaposlenih na bilo koji način osim direktnog posmatranja i uključuje upotrebu računara, telefona, žica, radija, kamera, elektromagneta, foto-elektronike ili foto-optičkih sistema, ne uključujući prikupljanje podatka u zajedničkim prostorijama poslodavca za javnu upotrebu, ili bilo koju aktivnost koja je zabranjena državnim ili saveznim zakonom.[14]

8 *Ibidem*.
9 Sl. glasnik RS, br. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009 i 111/2009, 121/2012, 104/2013 i 108/2014.
10 U čl. 153 KZ navedeno je da se gonjenje za krivična dela iz navedenih članova zakonika preduzimaju po privatnoj tužbi.
11 R. Filipović, *Teorija jezika i kontakti*, Zagreb, 2005, str. 17.
12 B. Francuski, Anglicizmi u informatičkoj i medijskoj leksici u srpskom, *Komunikacija i kultura online*, godina III, broj 3, 2012, str. 202.
13 OTA (Office for Technology Assesment), US Congres, The electronic Supervisor: *New technology, New Tensions*, Washington, DC, 1987, str. 27.
14 Public act no. 98–142, section 31–48d, Connecticut department of labor.

Terminu *electornic monitoring* značenje se definiše i kroz isticanje tri različita koncepta nadzora zaposlenih. Najpre, on uključuje upotrebu elektronskih uređaja za pregled i evaluaciju izvršavanja radnih obaveza (na primer, poslodavac može da ima uvid u *e-mail* poruke zaposlenog koje su primljene od kupca ili kupcu upućene, kako bi se pratio njegov učinak kao radnika zaduženog za tehničku podršku). Drugo, on uključuje *electornic surveillance* (elektronski nadzor), odnosno upotrebu elektronskih uređaja za posmatranje aktivnosti zaposlenih dok oni ne vrše aktivnosti koje su direktno vezane za obavljanje radnih zadataka ili iz nekog drugog razloga koji nije u vezi sa merenjem njihovog učinka kao zaposlenog (na primer, poslodavac može vršiti elektronski nadzor zaposlenog kao deo istrage u slučaju žalbe za seksualno uznemiravanje). Treće, termin podrazumeva korišćenje specijalizovanih forenzičkih alata za vraćanje i rekonstrukciju elektronskih podataka nakon brisanja, prikrivanja ili pokušaja uništavanja tih elektronskih podataka (na primer, poslodavac može koristiti specijalizovan softver da bi preuzeo, odnosno rekonstruisao izbrisane *e-mail* poruke koje se odnose na istragu navodne krađe njegovih poslovnih tajni).[15]

U australijskom Zakonu o privatnosti na radnom mestu, usvojenom 2011. godine, koji reguliše prikupljanje podataka i korišćenje uređaja za prismotru, odnosno nadzor radnika, terminom „nadzor" obuhvaćena je upotrebu uređaja za nadzor, koji obuhvataju optičke uređaje ili uređaje za praćenje (elektronski uređaj za određivanje pozicije osobe ili predmeta u geoprostoru), odnosno uređaja koji predstavlja kombinaciju optičkog uređaja i uređaja za praćenje.[16]

U pojedinim državama, kao na primer u Bugarskoj, poslodavac može koristiti tehnike elektronskog nadzora isključivo uz pristanak zaposlenih, koji taj pristanak treba da daju pre nego što postanu predmet nadzora (na primer, uz klauzulu u Ugovoru o radu). Pristanak mora biti dovoljno jasan, i zasnivati se na dobroj informisanosti zaposlenih. U slučaju spora, poslodavac je taj koji mora dokazivati da su zaposleni slobodno i bez ikakvih spoljnih faktora prinude pristali da se nad njima vrši nadzor. U Češkoj, upotreba elektronskih nadzornih tehnika moguća je samo u situacijama koje su predviđene Zakonom o radu[17]. Ukoliko zakonom predviđeni uslovi nisu ispunjeni, nadzor se neće smatrati dozvoljenim ni u slučaju da se zaposleni složio sa njegovim vršenjem.[18]

15 G. Lasprogata; J. N. King; S. Pillay, Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the Europe an Union, United States and Canada, *Stan. Tech,* L. Rev. 4, 2004, at para. 18. U ovom radu termini *monitoring* i *surveillance* se koriste naizmenično, odnosno kao sinonimi.

16 Workplace privacy act 2011, A2011-4.

17 U Zakonu o radu Češke Republike (Zákoník práce – No. 262/2006), u članu 316 (1), navodi se da zaposleni neće koristiti sredstva poslodavca, uključujući računare ili telekomunikacionu opremu za ličnu upotrebu, bez saglasnosti poslodavca. Kako bi pratio da li se ovo poštuje, poslodavac ima pravo da vrši nadzor nad zaposlenima. U članu 316 (2) propisuje se da poslodavac bez postojanja opravdanog razloga za praćenje ne može da zadire u privatnost zaposlenih na radnom mestu i u zajedničkim prostorijama poslodavca otvorenim ili prikrivenim nadzorom, presretanjem (uključujući i snimanje) njihovih telefonskih poziva, kao i proverom elektronske pošte ili poštanskih pošiljki. U slučaju da postoje opravdani razlozi za nadzor zaposlenog, poslodavac je dužan da o tome obavesti zaposlenog.

18 Privacy protection in the workplace – Guide for employees (Zaštita privatnosti na radnom mestu – vodič za zaposlenike), preuzeto sa: http://www.azop.hr/page.aspx?PageID=130, dostupno 4. 7. 2015.

Sredstva i metode elektronskog nadzora zaposlenih su brojne i raznovrsne i obezbeđuju poslodavcu informacije o različitim aspektima angažovanja tehnoloških i ljudskih resursa, a time i pojačanu kontrolu radnog procesa. Ovim vidom nadzora moguće je identifikovati problematična mesta, utvrditi proizvodna kašnjenja ili uvideti koji radnici rade „ispod proseka".[19] Iako poslodavci na raspolaganju imaju brojne sisteme za nadzor radnika, najčešće korišćeni su nadzor računara (meri broj otkucaja na tastaturi, brzinu i preciznost, a takođe je moguće koristiti i programe za uvid u ostale aktivnosti zaposlenog na računaru, uvid u sadržaj na njemu i sl.), nadzor *e-mail*-a i internet stranica (uvid u poslate i primljene poruke, njihov sadržaj i sl., kao i uvid u posećene internet stranice, i eventualnu zabranu posećivanja određenih stranica, poput zabrane posećivanja sajtova sa seksualnim sadržajem), video-nadzor (detektovanje krađa zaposlenih i neželjenog, odnosno nedopustivog ponašanja), praćenje i prisluškivanje.[20]

Brojni su i razlozi oslanjanja poslodavaca na elektronske uređaja za nadzor radnika. Kao ključni, izdvajaju se:

– praćenje produktivnosti (uključujući ograničavanje upotrebe resursa kompanije za ličnu upotrebu);
– zaštita od eventualnih sporova između radnika i poslodavca i obezbeđenje dokaza (na primer u slučaju tužbe za seksualno uznemiravanje, diskriminaciju, povredu autorskih prava, kleveta sl.);
– praćenje usklađenosti aktivnosti radnika sa politikom radnog mesta (praćenje upotrebe računara, interneta i upotreba elektronske pošte);
– sprečavanje ili otkrivanje povreda tajnosti;
– sprečavanje ili odgovor na neovlašćeni pristup (uključujući i hakovanje u korporativnu računarsku mrežu);
– ograničenje pristupa internetu;
– praćenje vozila;
– veća zaštita zaposlenih.[21]

S obzirom na intenzivan razvoj tehnologije, danas je dosta teško izvršiti pregled svih mogućih metoda i sredstava za nadzor. Stoga će u nastavku teksta biti ukazano na trenutno najaktuelnije oblike nadzora zaposlenih, a to su video-nadzor, nadzor i/ili snimanje telefonskih razgovora, praćenje elektronske pošte i internet saobraćaja i GPS praćenje. Naročita pažnja će biti posvećena video-nadzoru, jednom od najčešćih vidova nadzora radnog prostora.

19 M. J. Smith; B. J. Amick, *Electronic Monitoring* in the *Workplace*: *Implications for Employee Control and Job Stress*, in S. L. Sauter, J. J. Hurrell, Jr., and C. L. Cooper (eds), *Job Control and Worker Health*, Chichester. UK: John Wiley and Sons, Ltd., 1989, str. 276.
20 J. M. Mishra; S. M. Crampton, Employee monitoring: Privacy in the workplace?, *S.A.M. Advanced Management Journal*, Summer 98, Vol. 63 Issue 3, 1998, str. 4.
21 M. R. Bueckert, Electronic Employee Monitoring: Potential Reform Options. *The Law of Employee Monitoring in Canada*, Lexis Nexis Canada, 2009, str. 99–115.

1.1. Video-nadzor

Uprkos činjenici da se video-nadzor (sistem video-nadzora) godinama unazad koristi kao jedan od vidova zaštite imovine i da je njegova upotreba široko rasprostranjena, u literaturi se mogu naći samo opisne definicije pojma video-nadzora (sistem video-nadzora). Video-nadzor se definiše kao televizijski sistem u okviru koga se signal ne distribuira široj javnosti, već ograničenom krugu subjekata koji putem praćenja signala na monitorima vrše nadzor i druge bezbednosne funkcije na određenom području,[22] odnosno kao funkcionalno povezana tehnička sredstva koja primajući, prenoseći, obrađujući, arhivirajući i pregledajući snimljene zapise (slike) omogućavaju vizuelno posmatranje i nadzor, a kasnije i analizu aktivnosti u zaštićenim prostorijama.[23] S obzirom na to da ono što kamere beleže može posmatrati samo ograničeni broj lica, za označavanje sistema video-nadzora uobičajeno je korišćenje skraćenice CCTV (*closed circuit television* – televizija za zatvorenog kruga).[24]

Upotreba složenih sistema video-nadzora u zaštiti privatnog i javnog prostora započeta je krajem šezdesetih godina dvadesetog veka i to u sklopu mera čiji je cilj bio stvaranje uslova za sigurnije ulaganje kapitala i očuvanje političkih i ekonomskih interesa, kao i radi pojačavanja kontrole i nadzora u cilju što adekvatnijeg odgovora na kriminal. [25] Danas je primena sistema video-nadzora sve prisutnija u brojnim oblastima, pa i u obezbeđivanju objekata, nadzora saobraćaja i dobijanju video-zapisa ljudskih aktivnosti. Sistemi video-nadzora iz godine u godinu se usavršavaju i postaju sve pristupačniji široj populaciji. Uz sve prisutniju primenu sistema video-nadzora, sve češće se širom sveta ističe i zabrinutost u pogledu njegovog negativnog uticaja na privatnost građana.[26]

Sistem video-nadzora postaje deo integrisanog sistema zaštite kuća, stanova, malih i srednjih poslovnih prostora, galerija, banaka, pošta i sl., a sve češće podrazumeva i formiranje video-zapisa i arhiviranje događaja u prostoru koji se nadzire. Sastoji se iz:

- potrebnog broja spoljašnjih i unutrašnjih kamera, zavisno od geometrije objekata, mogućih prilaza, rasporeda prostorija koje treba nadgledati;
- odgovarajućih objektiva, sa ručnim ili automatskim podešavanjem otvora blende;
- kablova, koji služe za prenos video-signala, kada je u pitanju žična kamera;
- uređaja za prenos video-signala, kada je u pitanju bežična kamera;
- centralnih uređaja, koji služe za obradu i arhiviranje slika dobijenih putem kamera;
- uređaja za prikaz slike;
- operatera.[27]

22 A. R. Matchett, CCTV for security professionals, *Burligton: Elsevier Science*, 2003, str. 236.
23 R. Golob, *Sistemi zaščite in varovanja oseb in premoženja,* Ljubljana, R. Golob,1997, str. 214.
24 V. Damjanovski, *CCTV networking and digital technology*, Oxford: Butter-worth-Heineman, 2005, str. 501.
25 N. Fajf; Dž. Banister, Oči uprete u ulicu, CCTV nadzor i grad, *Prizori ulice*, Beograd, 2002, str. 354.
26 Preuzeto sa: http://whatis.techtarget.com/definition/closed-circuit-television-CCTV, dostupno 5. 7. 2015.
27 S. Vuković, *Prevencija kriminala,* Beograd, 2010, str. 136.

Instalacija sistema video-nadzora u radnom prostoru može predstavljati vid zaštite od raznih prekršajnih i kriminalnih radnji zaposlenih i drugih lica, kao i vid zaštite radnika i mera za zaštitu imovine i unapređenje produktivnosti (kontrola obavljanja posla i tehnoloških procesa), a može se koristiti i kao dokaz u slučaju spora između poslodavca i zaposlenog.

Kao prepreke u primeni sistema video-nadzora poslovnog prostora, mogu se izdvojiti: psihološki pritisak na zaposlene, mogućnost zloupotrebe snimljenog materijala, zadiranje u privatnost zaposlenih i narušavanje njihovog dostojanstva. Uprkos činjenici da poslodavci sve češće uređuju način korišćenja i čuvanja podataka koji su dobijeni video-nadzorom, pribavljaju saglasnost zaposlenih i upoznaju ih sa svrhom uvođenja video-nadzora i pravilima korišćenja, navedene prepreke mogu postojati.

U studiji AMA navodi se da je skoro polovina (48%) kompanija koje su bile obuhvaćene istraživanjem, 2007. godine upotrebljavala video-nadzor u borbi protiv krađa, nasilja i sabotaža (u odnosu na 33% u 2001. godini). Samo 7% upotrebljavalo je video-nadzor za praćenje procesa rada zaposlenih, što predstavlja neznatno povećanje u odnosu 4% u 2001. godini. Većina poslodavaca obaveštavala je zaposlene o primeni sistema video-nadzora (njih 78% u slučajevima primene u cilju sprečavanja krađa, odnosno njih 89% kada je sistem video-nadzora usmeren ka merenju učinka radnika).[28]

Za video-nadzor radnog okruženja mogu se koristiti različite vrste kamera, od onih koje su jasno vidljive svima, do onih koji se kamufliraju u razne predmete (časovnik, sliku, radio i sl.) i koje se mogu podvesti pod sredstva tajnog video-nadzora. Pitanje dozvoljenosti primene mera video-nadzora u poslovnim prostorijama posebno dobija na značaju kada se on realizuje postavljanjem skrivenih kamera. Odgovori zakonodavaca su različiti. U Nemačkoj je, primera radi, tajni video-nadzor u preduzećima dozvoljen u slučajevima kada treba otkriti ili sprečiti dalje vršenje krivičnih dela ili prekršaja. Istovremeno, u slučaju zloupotreba, predviđena je kazna zatvora do jedne godine ili novčana kazna.[29]

Prema mišljenju nemačkog Saveznog radnog suda, tajni video-nadzor zaposlenog dozvoljen je: ukoliko se sumnja na krivično delo ili drugo masovno kršenje propisa od strane zaposlenog na štetu poslodavca, ukoliko sve blaže metode istraživanja nisu dale rezultate, ukoliko je tajni video-nadzor jedino rešenje da se problem reši i ukoliko primena nije nesrazmerna. U takvim slučajevima, nadzor mora da se koncentriše na zaposlenog za koga se pretpostavlja da krši propise ili čini krivično delo i na mesta gde se očekuje da se krivično delo ili drugo kršenje propisa dešava (na primer kasa).[30]

Poseban zakon o video-nadzoru ne postoji u svim državama Evropske unije, a brojna pitanja koja se mogu dovesti u vezu sa njim regulisana su drugim propisima. Tako su npr. u Finskoj u Krivičnom zakoniku[31] prisutne odredbe

28 The Epolicy Institute, 2007 Electronic Monitoring & Surveillance Survey, dostupno na: http://www.epolicyinstitute.com/2007-survey-results (1. 7. 2015).

29 Preuzeto sa: http://www.parlament.gov.rs/upload/archive/files/lat/doc/istrazivanja/Pravni%20okvir%20za%20primenu%20video%20nadzora%20lat.docx, *dostupno 15. 7. 2015.*

30 Preuzeto sa: http://www.taylorwessing.com/globaldatahub/article_cctv_germany.html, dostupno 16. 7. 2015.

31 The Criminal Code of Finland (39/1889, sa amandmanima do 927/2012), preuzeto sa: http://

kojima se zabranjuje nezakonita upotreba elektronskog nadzora i prisluškivanja, a relevantne odredbe sadrže i Zakon o ličnim podacima.[32] Zakon o zaštiti privatnosti na radu[33] sadrži odredbe kojima se definišu pojedina pravila primene video-nadzora na radnom mestu. U poglavlju koji uređuje ovo pitanje navodi se da poslodavac može koristiti kamere i nadzor u radnim prostorijama u cilju obezbeđivanja lične sigurnosti zaposlenih i drugih lica u prostorijama, ako štiti imovinu ili nadzire ispravnost proizvodnih procesa, kao i za sprečavanje ili istragu situacija kojima se ugrožavaju bezbednost imovine ili proizvodni procesi. Kamera koja se koristi za nadzor mora biti jasno vidljiva, a znaci u vezi sa video-nadzorom i načinom sprovođenja moraju biti istaknuti u prostorijama u kojima se nalaze kamere. Zakonom o ličnim podacima, precizirano je da nadzor kamerama, nezavisno od toga gde se odvija, mora biti opravdan u dovoljnoj meri. Nepotrebno snimanje podataka je zabranjeno, a lica koja su u prostorijama moraju biti svesni nadzora, tako da se mogu ponašati u skladu sa njim.

U izveštaju studije „Zaštita ličnih podataka radnika: slučaj nadzora i praćenja" sprovedenoj u zemljama Evropske unije finansiranoj od strane Evropske komisije i Generalnog direktorata za zapošljavanje i socijalna pitanja, po pitanju nadzora i praćenja zaposlenih navedeno je da, uopšteno govoreći, upotrebu kamera za nadzor treba smatrati zakonitom. Dalje je navedeno da je upotreba video-nadzora u radnom okruženju zakonita ukoliko se nadzor primenjuje radi zaštite zdravlja i bezbednosti, zaštite imovine poslodavca, praćenje procesa proizvodnje i praćenja radnog učinka. Praćenje ne bi trebalo da bude trajno, nadzor se ne sme vršiti u privatnim oblastima (kupatila i sl.) i tajni video-nadzor je dozvoljen u veoma ograničenim slučajevima (npr. ukoliko postoje osnovi sumnje da postoje ozbiljna kršenja propisa).[34]

Kada je u pitanju praksa Evropskog suda za ljudska prava po pitanju povreda prava na privatnost u slučaju video-nadzora na radnom mestu, u slučaju Kopke protiv Nemačke (*Köpke v. Germany* – 420/07 od 5. 10. 2010),[35] sud je zaključio

www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf, dostupno 19. 6. 2015.

32 Personal data act of Finland (523/1999), preuzeto sa: http://www.finlex.fi/en/laki/kaannokset/1999/en19990523.pdf, dostupno 19. 6. 2015.

33 Act on the Protection of Privacy in Working Life (759/2004), preuzeto sa: http://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf, dostupno 19. 6. 2015.

34 Preuzeto sa: http://ec.europa.eu/social/BlobServlet?docId=2507&langId=en, dostupno 13. 6. 2015.

35 Podnosilac predstavke, Karin Kopke, bila je radnica, blagajnik u supermarketu i otpuštena je zbog navodne krađe, a kao dokaz poslodavac je priložio snimak sa video-nadzora koji je pribavljen uz pomoć detektivske agencije. Video-nadzor podnosioca predstavke je sproveden bez prethodnog upozorenja od strane poslodavca. Snimci koji su na taj način dobijeni pregledani su od strane nekoliko zaposlenih i korišćeni su kasnije u sudskim postupcima u zemlji. Na ovaj način, snimci su postali dostupni javnosti, a podnosilac predstavke pozvala se na povredu člana 8 Konvencije, odnosno na to da joj je neovlašćenim snimanjem povređeno pravo na privatnost. S druge strane, poslodavac je isticao da su preduzete mere bile vremenski ograničene na dve nedelje i da je snimano samo područje gde je podnosilac predstavke radila. Snimci koji su dobijeni korišćeni su od strane ograničenog broja lica koji su zaposleni kod istog poslodavca i sve isključivo radi dokazivanja nezakonitog ponašanja zaposlene, kao i radi vođenja sporova pred nadležnim sudovima. Suštinsko pitanje na koje je trebalo dati odgovor jeste da li je država Nemačka na adekvatan način omogućila zaštitu prava na privatnost podnosioca predstavke, u kontekstu video-nadzora na radnom mestu. U ovom slučaju, pored prava na zaštitu privatnosti, trebalo je uzeti u obzir i pravo na zaštitu svojine. Predstavka je odbačena kao neosnovana, u skladu sa članom 35 st. 3 i 4 Konvencije. (Preuzeto sa: http://hudoc.echr.coe.int/eng?i=001-

da u ovom slučaju ne postoji ništa što bi ukazivalo na to da su domaći organi propustili da zaštite pravičnu ravnotežu, između prava podnosioca predstavke na poštovanje njenog privatnog života po čl. 8 Konvencije za zaštitu ljudskih prava i osnovnih sloboda (u daljem tekstu Konvencija) i interesa poslodavca u zaštiti imovinskih prava i javnog interesa u pravilnom sprovođenju pravde. Obrazlažući presudu, sud je naveo da se tajni video-nadzor zaposlenog na radnom mestu smatra značajnim zadiranjem u privatni život zaposlenog; međutim, takođe je navedeno i da je tajni video-nadzor zaposlenog sproveden tek nakon što je poslodavac primetio nepravilnosti na računima, da je bio vremenski ograničen i da je bio ograničen u pogledu prostora koji je video-nadzor pokrivao. U skladu sa tim, sud je zaključio da je, na taj način, mešanje u privatni život podnosioca predstavke bilo ograničeno isključivo na ono što je bilo potrebno, kako bi se postigli ciljevi kojima se težilo sprovođenjem tajnog video-nadzora. Takođe je uzeta u obzir i činjenica da je tajni nadzor poslužio i kao sredstvo da se sa ostalih zaposlenih, koji nisu bili krivi za bilo koje krivično delo, obriše sumnja. I na kraju, sud je konstatovao da nije bilo nijednog drugog jednako efikasnog sredstva za zaštitu imovinskih prava poslodavca koji bi se u manjoj meri mešali u poštovanje privatnog života podnosioca predstavke. Presuda je zaključena komentarom da ovako suprotstavljeni interesi u budućnosti mogu dobiti drugačiju težinu, imajući u vidu činjenicu da je sve više i više sofisticiranih tehnologija kojima se može zadirati u privatnost.

U državama regiona pitanje primene video-nadzora tretirano je u zakonskim i podzakonskim aktima koji regulišu različite oblasti. Primera radi, u Bosni i Hercegovini pitanje primene video-nadzora uređeno je članom 21a Zakona o zaštiti ličnih podataka[36] kojim se reguliše pitanje obrade ličnih podataka putem video-nadzora. Ovim članom je regulisano da snimci pohranjeni putem video-nadzora na određenom prostoru na osnovu kojih se može identifikovati nosilac podataka predstavljaju zbirku ličnih podataka, a da je kontrolor koji vrši video-nadzor dužan doneti odluku koja će sadržati pravila obrade s ciljem poštovanja prava na zaštitu privatnosti i ličnog života nosioca podataka. Predviđena je i obaveza kontrolora koji vrši nadzor da na vidnom mestu istakne obaveštenje o vršenju nadzora i kontakt putem kojeg se mogu dobiti pojedinosti o video-nadzoru. U Republici Hrvatskoj oblast video-nadzora uređena je Pravilnikom o načinu i uslovima obavljanja poslova privatne zaštite na javnim površinama[37], a sam Pravilnik ne sadrži nijednu odredbu koja se tiče video-nadzora u službenim i poslovnim prostorijama. Za razliku od Bosne i Hercegovine, koja ovo pitanje reguliše gore pomenutim Zakonom, i Srbije koja ovu oblast uopšte nije regulisala, u Hrvatskoj je ovo pitanje regulisano Zakonom o radu[38], kojim je propisano da se poslodavac pre uvođenja novih tehnologija, a ovo uključuje i uvođenje video-nadzora, mora posavetovati sa predstavnicima radnika.

U Republici Srbiji nisu usvojene zakonske odredbe koje na sveobuhvatan način uređuju pitanje video-nadzora u kontekstu obrade i zaštite ličnih podataka. Iako su uslovi za prikupljanje i obradu podataka o ličnosti, prava lica i zaštita prava

101536#{%22itemid%22:[%22001-101536%22]}, dostupno 4. 7. 2015).
36 *Sl. glasnik BiH*, br. 49/06, 76/11 i 89/11.
37 *Narodne novine*, br. 36/12.
38 *Narodne novine*, br. 93/14.

lica čiji se podaci prikupljaju i obrađuju, ograničenja zaštite podataka o ličnosti, postupak pred nadležnim organom za zaštitu podataka o ličnosti, obezbeđenje podataka, evidencija i iznošenje podataka iz Republike Srbije uređeni Zakonom o zaštiti podataka o ličnosti,[39] ovaj zakon ni u jednoj odredbi ne uređuje obradu ličnih podataka građana putem video-nadzora.

Predloženim izmenama i dopunama navedenog zakona,[40] pored definisanja pojma video-nadzora, predviđeno je i uređenje prava i obaveze kako poslodavca, tako i radnika sa njim u vezi. U tekstu predloga, video-nadzor je definisan kao svaki sistem koji se koristi za snimanje određenog javnog, službenog i radnog prostora, bez obzira na to da li omogućava samo nadzor ili i pohranjivanje tako sačinjenih video-zapisa i njihovo prenošenje putem računarske mreže.

Predlog sadrži i posebne odredbe koje se tiču video-nadzora pristupa u službene i poslovne prostorije i video-nadzora u službenom i poslovnom prostoru. U članu 34 predloga navodi se da rukovalac podacima može da vrši nadzor pristupa u službene ili poslovne prostorije, ukoliko je to neophodno radi bezbednosti lica i imovine, kontrole ulaska ili izlaska iz službenog ili poslovnog prostora ili, ako zbog prirode posla, postoje mogući rizici za zaposlene. Odluku o uvođenju video-nadzora rukovalac podacima mora doneti u pisanoj formi. Ova odluka mora da sadrži razloge za uvođenje video-nadzora, ukoliko uvođenje video-nadzora nije propisano zakonom, a zaposleni koji rade u prostoru koji je pod video-nadzorom moraju biti obavešteni o tome. Video-nadzor nije dozvoljen u službenom i poslovnom prostoru van radnog mesta, naročito u garderobama, liftovima i sanitarnim prostorijama.

Na osnovu do sada navedenog mogu se izvesti brojne zajedničke odlike primene video-nadzora od strane poslodavaca. Oni ga koriste kako bi nadgledali i pospešivali produktivnost zaposlenih, njihovu bezbednost i bezbednost radnog okruženja, sprečili njihovo nedozvoljeno i kažnjivo ponašanje, ali i u sklopu mera prevencije od ugrožavanja drugih lica, tj. kao metod odvraćanja od krađe i drugih krivičnih dela. Konkretni ciljevi i domašaji primene video-nadzora uslovljeni su specifičnostima objekata na kojima se/u kojima se video-nadzor realizuje (npr. u bankama i menjačnicama video-nadzor koristiti kako bi se potencijalni izvršilac odvratio od napada na zaštićeni objekat, a ukoliko je do razbojništva ipak došlo, snimci sa video-nadzora mogu biti značajan dokaz u postupku njegovog otkrivanja, rasvetljavanja i dokazivanja).

Kao osnovna načela primene video-nadzora u radnom okruženju mogu se izdvojiti legitimnost, srazmernost, nužnost i transparentnost. Načelo legitimnosti podrazumeva da se svaka obrada ličnih podataka mora obavljati na zakonit način, uz poštovanje dostojanstva i privatnosti zaposlenih, a da se podaci obrađuju isključivo u cilju zaštite imovine poslodavca. Načelo srazmernosti podrazumeva da lični podaci koji se obrađuju moraju biti relevantni i ne prekomerni, s obzirom na svrhu obrade. Primera radi, u slučaju da se sumnja da zaposleni krade novac iz kase, nadzor bi trebalo ograničiti vremenski i na određenog zaposlenog ili na

39 *Sl. glasnik RS*, br. 97/2008, 104/2009 – dr. Zakon, 68/2012 – odluka US i 107/2012.

40 Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti pripremio je model Zakona o zaštiti podataka o ličnosti i otvorio javnu raspravu o njemu u junu 2014. godine. Model zakona preuzet je sa http://www.poverenik.rs/images/stories/model-zakona/modelzzpl.docx, dostupno 4. 8. 2015.

određene oblasti (izbegavati kontinuiran i automatski nadzor). Načelo nužnosti bi podrazumeva prethodnu procenu mogućnosti ostvarivanja konkretnih ciljeva primenom manje invazivnih metoda nadzora, odnosno utvrđivanje da te metode nadzora nisu moguće, odnosno dovoljne. Načelo transparentnosti podrazumeva da je video-nadzor jasan i otvoren i da su zaposleni obavešteni o tome kada se video-nadzor primenjuje, a da se tajni nadzor može primenjivati samo u slučajevima kada je dozvoljen zakonom i posebnim propisima, odnosno odobren od strane nadležnog organa (najčešće suda). Treba napomenuti i to da značaju ulogu u sistemu video-nadzora imaju i zaposleni koji obavljaju poslove operatera ili administratora sistema (rukovalac, kontrolor). Svi oni treba da poštuju propise o čuvanju i obradi ličnih podataka, kao i načelo čuvanja službene, odnosno poslovne tajne.

1.2. Nadzor telefonskih komunikacija

Detalji o telefonskim pozivima zaposlenih, kao i sami razgovori mogu biti snimljeni tokom nadzora. Tačan broj razgovora i vreme trajanje svakog poziva, kao i vreme provedeno između poziva, mogu se automatski beležiti kako bi se kasnije analizirali.[41]

U izveštaju AMA, navodi se da vreme trajanja poziva i pozvane brojeve beleži 45% kompanija, dok 16% kompanija snima telefonske razgovore. O nadzoru telefonskih komunikacija zaposlene je obavestilo 84% poslodavaca, a njih 6% je otpustilo zaposlene zbog neadekvatne, tj. privatne upotrebe kancelarijskog telefona.[42]

1.3. Elektronska pošta i internet

U današnje vreme, upotreba interneta i elektronske pošte u većini kompanija postaje deo radnih obaveza. U ovom kontekstu posmatrano, bitno je praviti razliku između poslovnih i privatnih *e-mail* adresa. Nadziranje elektronske pošte i interneta u korist poslodavca, automatski podrazumeva i obradu ličnih podataka, a ovo dalje podrazumeva i zaštitu privatnosti zaposlenog. U nekim zemljama, poput Hrvatske i Češke, poslodavci moraju obavestiti zaposlene o nadgledanju i nadziranju elektronske pošte. U drugim, poput Bugarske i Poljske, ova obaveza nije zakonom ustanovljena.[43]

U izveštaju AMA, od 43% kompanija koje prate elektronsku poštu, njih 96% prati spoljni saobraćaj (ulazne i izlazne poruke), dok samo 58% nadzire interne poruke koje se šalju između zaposlenih. Kada je u pitanju metoda praćenja, 73% organizacija koriste programe za automatsko praćenje elektronske pošte, dok 40% poslodavaca određuje jednu osobu da ručno čita i pregleda elektronsku poštu. O nadzoru elektronske pošte zaposlene obaveštava 71% kompanija.[44]

41 Preuzeto sa: http://www.ap.org/Content/AP-In-The-News/2013/Govt-obtains-wide-AP-phone-records-in-probe, dostupno 3. 7. 2015.

42 The Epolicy Institute, 2007 Electronic Monitoring & Surveillance Survey, dostupno na: http://www.epolicyinstitute.com/2007-survey-results (1. 7. 2015).

43 Privacy protection in the workplace – Guide for employees (Zaštita privatnosti na radnom mestu – vodič za zaposlenike), preuzeto sa: http://www.azop.hr/page.aspx?PageID=130, dostupno 4. 7. 2015.

44 The Epolicy Institute, 2007 Electronic Monitoring & Surveillance Survey, dostupno na: http://

Kada je u pitanju nadzor interneta, od 66% kompanija koje nadziru upotrebu interneta, 65% kompanija koriste programe za blokiranje konekcija ka nedozvoljenim/neadekvatnim internet sajtovima (96% blokira pristup sajtovima sa sadržajima za odrasle, 61% blokira pristup sajtovima za igrice, 50% blokira pristupe društvenim mrežama itd.).[45]

1.4. GPS nadzor

Razvoj uređaja koji omogućavaju praćenje i određivanje geolokacije omogućio je poslodavcima praćenje zaposlenih čije radno okruženje nije statično, tj. onih koji radno vremena provodi u vozilu koje je u vlasništvu poslodavca. Poslodavcu je na ovaj način omogućeno da u svakom trenutku može saznati lokaciju na kojoj se zaposleni nalazi sa službenim vozilom.

2. Zaštita ličnih podataka i privatnosti na radnom mestu u pravu Evropske unije

Pravo na privatnost predstavlja elementarno ljudsko pravo, kako međunarodno, tako i ustavno pravo javno-pravnog značaja, kao jedan od nezamenjivih elemenata čovekovog postojanja koji štiti od prekomernog zadiranja državne vlasti, javnosti i drugih pojedinaca u nečiju duševnu, prostornu i informacijsku privatnost.[46] Danas postoje brojna sofisticirana tehnička sredstva koja imaju ogromne mogućnosti primene u nadgledanju ljudi u gotovo svim aspektima njihovog života i rada. Istovremeno, sa razvojem tehnologije, pravo na tajnost pisama i drugih sredstava komunikacije, kao i zaštita ljudskog imuniteta u najširem smislu, proklamuje se pravnim normama najveće pravne snage, i predstavlja centralni deo korpusa ljudskih prava konstituisanih tokom druge polovine XX veka.[47] Univerzalna deklaracija o ljudskim pravima Ujedinjenih nacija iz 1948. u članu 12 utvrdila je da „niko ne može biti izložen proizvoljnom mešanju u privatni život, porodicu, stan, prepisku, niti napadima na čast i ugled". U Međunarodnom paktu o građanskim i političkim pravima iz 1966. u članu 17 kaže se da „niko ne može biti predmet samovoljnih ili nezakonitih mešanja u njegov privatni život, u njegovu porodicu, u njegov stan ili njegovu prepisku, niti nezakonitih povreda nanesenih njegovoj časti ili njegovom ugledu". Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda iz 1950. u članu 8 kaže da „svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske". Univerzalna deklaracija govori o zabrani proizvoljnog mešanja u privatni život, a Međunarodni pakt govori i o samovoljnom i o nezakonitom

www.epolicyinstitute.com/2007-survey-results (1. 7. 2015).
45 *Ibidem*.
46 M. Boban, Pravno na privatnost i pravno na pristup informacijama u savremenom informacijskom društvu, *Zbornik radova Pravnog fakulteta u Splitu*, god. 49, 3/2012, Pravni fakultet – Sveučilište u Splitu, 2012, str. 582.
47 D. Marinković, *Suzbijanje organizovanog kriminala – specijalne istražne metode*, Prometej, Novi Sad, 2010, str. 509.

mešanju, što podrazumeva dopuštenost zakonitog mešanja, tj. prava suverenih država da samostalno nacionalnim zakonodavstvom urede slučajeve i uslove u kojima je moguć zakoniti prodor u sferu lične slobode u cilju zaštite slobode i bezbednosti drugih lica, društva ili potreba krivičnog postupka.[48] U društvu u kojem živimo, zahtev za poštovanje ljudskih prava dostigao je univerzalnu prihvaćenost, a stepen i način njihove zaštite predstavljaju jedan od ključnih kriterijuma na osnovu kojih se mere nivo demokratičnosti nekog društva i stepen njihove civilizovanosti.[49]

Osnovni pravni okvir o elektronskom nadzoru zaposlenih na radnom mestu, u zemljama Evropske unije, predstavljaju pravna načela Saveta Evrope i direktive Evropske unije o elektronskom nadzoru zaposlenih na radnom mestu. Članom 8 Konvencije propisano je da svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske, da se javna vlast ne meša u vršenje ovog prava, osim ako je takvo mešanje predviđeno zakonom i ako je to neophodna mera u demokratskom društvu u interesu nacionalne bezbednosti, javne sigurnosti, ekonomske dobiti zemlje, sprečavanja nereda ili sprečavanja zločina, zaštite zdravlja i morala ili zaštite prava i sloboda drugih.

Od 1992. godine, Evropski sud za ljudska prava, kroz odluku o slučaju *Niemietz v. Germany* (13710/88 od 16. 12. 1992),[50] proširio je definiciju da privatni život i prepiska uključuju i poslovne odnose, s obzirom na to da u presudi navodi da pravo na poštovanje privatnog života u izvesnoj meri sadrži i pravno na uspostavljanje i razvijanje odnosa sa drugima i da ne postoji nijedan razlog da se iz pojma „privatni život" isključe profesionalne ili poslovne aktivnosti. U ovom slučaju nije pravljena razlika između privatnih i poslovnih prepiski.

U slučaju *Halford v. UK Gov.* (20605/92 – od 25. 6. 1997)[51] Evropski sud za ljudska prava smatrao je da nadzor telefonskih poziva zaposlenog na radnom mestu od strane poslodavca predstavlja neopravdano mešanje u pravo zaposlenog na privatnost i prepisku. U ovom slučaju sud je smatrao da Konvencija članom 8 štiti svaku prepisku, nezavisno od toga o kojoj vrsti prepiske se radi (*e-mail*, faks, mobilna i fiksna telefonija i sl.). Ipak, bitno je napomenuti i to da je član 8 Konvencije primenjiv tek nakon što se pravni lekovi koji važe u domaćim zakonodavstvima i direktive EU o nadzoru zaposlenih iscrpe.

Da pravo zaposlenog na privatnost na radnom mestu nije apsolutno, govori i zaključak Evropskog suda za ljudska prava u slučaju *Benediktsdóttir v. Iceland* (38079/06 od 16. 6. 2009)[52], u kom se navodi da pravo na privatnost i prepisku mora biti uravnoteženo sa ostalim pravima, pre svega sa pravima poslodavca.

48 M. Živković, Tajnost pisama prema novom Ustavu Srbije i posebna dokazna radnja tajnog zvučnog i optičkog nadzora, *NBP – Nauka, bezbednost, policija, god. 11, br. 3/2006*, Kriminalističko-policijska akademija, Beograd, 2006, str. 3–16.

49 D. Simović, R. Zekavica, *Policija i ljudska prava*, Kriminalističko-policijska akademija, Beograd, 2012, str. 221

50 Preuzeto sa: http://hudoc.echr.coe.int/eng?i=001-58039#{%22itemid%22:[%22001-58039%22]}, dostupno 19. 7. 2015.

51 Preuzeto sa: http://hudoc.echr.coe.int/eng?i=001-58039#{%22itemid%22:[%22001-58039%22]}, dostupno 19. 7. 2015.

52 Preuzeto sa: http://hudoc.echr.coe.int/eng?i=001-93526#{%22itemid%22:[%22001-93526%22]}, dostupno 19. 7. 2015.

Jedna od prvih direktiva Evropske unije, a ujedno i jedan od najvažnijih pravnih instrumenata kojim se štite lični podaci na nivou Evropske unije, jeste Direktiva 95/46/EZ[53] Evropskog parlamenta i Veća o zaštiti fizičkih lica u pogledu postupanja sa ličnim podacima, čiji je cilj zaštita zagarantovanih prava i sloboda fizičkih lica, a pre svega, prava na privatnost pri obradi tih podataka. Među pravima i obavezama utvrđenim ovom direktivom, ističe se da lice o kome se prikupljaju lični podaci ima pravo da budu obavešteno o prikupljanju ličnih podataka. Direktivom je lični podatak definisan kao svaki podatak koji se odnosi na fizičko lice koje je identifikovano ili se može identifikovati. Lični podaci mogu se prikupljati i obrađivati samo u skladu sa zakonom, za tačno određenu svrhu i srazmerno svrsi prikupljanja. Iako se ova direktiva ne bavi direktno pitanjem nadzora poslodavca, nedvosmisleno se može zaključiti da u slučaju spornih pitanja u vezi sa nadzorom na radnom mestu, treba poštovati princip privatnosti. U skladu sa gore navedenim, može se zaključiti da poslodavci moraju da obezbede da vršenje nadzora bude legitimno i ograničeno, kao i da bude transparentno. Ovo bi dalje značilo da bi se bilo koje praćenje komunikacija i aktivnosti zaposlenih bez znanja zaposlenog ili njegovog pristanka, smatralo nezakonitim.

Druga važna direktiva koja se bavi pitanjem privatnosti i nadzorom elektronskih komunikacija jeste Direktiva EU 2002/58/EZ[54], koja se odnosi na obradu ličnih podataka i zaštitu privatnosti u javnom sektoru elektronskih komunikacija. Međutim, ova direktiva se konkretno bavi javnim mrežama i presretanjem komunikacija, što bi značilo da njom nije zaštićen nadzor privatnih komunikacija u okviru unutrašnjih (privatnih) mreža.

Trenutno, u Evropskoj uniji ne postoji poseban zakon u pogledu privatnosti i zaštite ličnih podataka zaposlenog na radnom mestu. Ipak, u članu 31 Povelje o osnovnim pravima Evropske unije[55], čija je primena obavezna kad god Države članice primenjuju pravo EU, navodi se da svaki radnik ima pravo na radne uslove kojima se poštuju njegovo zdravlje, bezbednost i dostojanstvo.

Na osnovu do sada navedenog može se zaključiti da u cilju sprečavanja zloupotreba poslodavci mogu da usvoje interne propise, da upoznaju zaposlene sa praksom kompanije da vrši elektronski nadzor, da obaveste zaposlenog ukoliko je pod nadzorom, kao i da mu omoguće uvid u njegove lične podatke koji su prikupljeni nadzorom. Nadzor ne bi smeo da se vrši u prostorijama poput svlačionica, toaleta, prostorija za odmor i sl., a podrazumeva se i zabrana prikupljanja ličnih podataka koji nisu u vezi za radnim obavezama.

53 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Official Journal, L 281, 23. 11. 1995, str. 31–50.

54 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); Official Journal L 201, 31. 7. 2002, str. 37–47.

55 Charter of fundamental rights of the European Union (2000/c 364/01); Official Journal of the European Communities C 364/1.

Zaključak

Više je nego jasno da elektronski nadzor radnog okruženja predstavlja bitan segment aktivnosti i mera koje poslodavci koriste kako bi zaštitili svoje poslovne interese i imovinu. Uz to, na ovaj način moguće je registrovanje i arhiviranje materijala koji zbog svoje prirode i sadržaja mogu biti od značaja za utvrđivanje činjenica u postupku koji povodom konkretnih događaja preduzimaju nadležni organi poslodavca, ali i drugi, pa i policija i organi krivičnog postupka. Razvoj tehnologije koji je omogućio proizvodnju, eksploataciju, stalnu nadogradnju i usavršavanje velikog broja uređaja i sistema elektronskog nadzora, uz brojne pozitivne efekte primene, za sobom povlači i pitanje mogućnosti, opravdanosti i dozvoljenosti kršenja prava na dostojanstvo i privatnost nadziranih osoba na njihovom radnom mestu. Sudska praksa Evropskog suda za ljudska prava (u slučaju *Köpke v. Germany*) ukazuje na činjenicu da privatnost na radnom mestu ima svoje granice, pa se može zaključiti da, kada je reč o zaštiti legitimnih interesa poslodavca, odnosno da se, ukoliko je izvršeno krivično delo ili prekršaj na štetu poslodavca, privatnost zaposlenog ne može garantovati.

Uz nužnost sveobuhvatnog normativnog regulisanja elektronskog nadzora zakonskim tekstom, pojedina pitanja bi se mogla dodatno urediti i internim aktima poslodavaca. Nadzor treba koristiti samo u slučaju ostvarivanja legitimnih ciljeva, on mora biti transparentan, srazmeran i nužan. Interni akti poslodavca treba da sadrže odredbe kojima se jasno definišu polje primene, ciljeve i razloge uvođenja sistema nadzora, a sa uvođenjem mera elektronskog nadzora morali bi se složiti i zaposleni.

Literatura

1. Boban, M.; *Pravno na privatnost i pravno na pristup informacijama u savremenom informacijskom društvu*, Zbornik radova Pravnog fakulteta u Splitu, god. 49, 3/2012, Pravni fakultet – Sveučilište u Splitu, Split, 2012.
2. Bueckert, R. M.; Electronic Employee Monitoring: Potential Reform Options, *The Law of Employee Monitoring in Canada*, Lexis Nexis, Canada, 2009.
3. Damjanovski, V.; *CCTV networking and digital technology*, Oxford: Butterworth-Heineman, 2005.
4. Fajf, N., Banister, Dž.; Oči uprete u ulicu, CCTV nadzor i grad, *Prizori ulice*, Clio, Beograd, 2002.
5. Filipović, R.; *Teorija jezika i kontakti*. Jugoslovenska akademija znanosti i umetnosti – Školska knjiga, Zagreb, 1986.
6. Francuski, B.; Anglicizmi u informatičkoj i medijskoj leksici u srpskom. *Komunikacija i kultura online*, godina III, broj 3, 2002.
7. Golob, R.; *Sistemi zaščite in varovanja oseb in premoženja*, R. Golob, Ljubljana, 1997.
8. Lasprogata, G., King, N., Pillay, S.; Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy

through a Comparative Study of Data Privacy Legislation in the Europe an Union, United States and Canada. Stan. Tech. L. Rev, 2004.

9. Marinković, D.; *Suzbijanje organizovanog kriminala – specijalne istražne metode*, Prometej, Novi Sad, 2010, str. 509.
10. Matchett, A. R.; CCTV for security professionals, Burligton: Elsevier Science, 2003.
11. Mishra, J. M.; Crampton, S. M.; Employee monitoring: Privacy in the workplace?, *S.A.M. Advanced Management Journal*, Summer98, Vol. 63 Issue 3, 1998.
12. Simović, D., Zekavica, R.; *Policija i ljudska prava*, Kriminalističko-policijska akademija, Beograd, 2012.
13. Smith, M. J.; Amick, B. J.; *Electronic Monitoring* in the *Workplace*: *Implications for Employee Control and Job Stress*, *Job Control and Worker Health*, Chichester, UK: John Wiley and Sons, Ltd., 1989.
14. Vuković, S.; *Prevencija kriminala*, Kriminalističko-policijska akademija, Beograd, 2010.
15. OTA (Office for Technology Assesment), US Congres, The electronic Supervisor: New technology, New Tensions, Washington, DC, 1987, str. 27.
16. Živković, M.; Tajnost pisama prema novom Ustavu Srbije i posebna dokazna radnja tajnog zvučnog i optičkog nadzora, *NBP – Nauka, bezbednost, policija 3/2006*, Kriminalističko-policijska akademija, Beograd, 2006.

Zakoni

17. *An act requiring notice to employees of electronic Monitoring by employers*, Connecticut department of labor, public act no. 98–142.
18. Charter of fundamental rights of the European Union (2000/c 364/01); Official Journal of the European Communities C 364/1.
19. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Official Journal, L 281, 23. 11. 1995, str. 31–50.
20. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002. concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); Official Journal L 201, 31. 7. 2002, str. 37–47.
21. *Krivični zakonik Republike Srbije*, „Službeni glasnik RS", br. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009 i 111/2009, 121/2012, 104/2013 i 108/2014.
22. *Personal data act of Finland*, 523/1999.
23. *Pravilnik o načinu i uslovima obavljanja poslova privatne zaštite na javnim površinama*, Narodne novine, br. 36/12.
24. *The Criminal Code of Finland*, 39/1889, sa amandmanima do 927/2012.
25. *Zakon o zaštiti ličnih podataka*, Sl. glasnik BiH, br. 49/06, 76/11 i 89/11.

26. *Zakon o radu*, Narodne novine, br. 93/14.
27. *Zakon o zaštiti podataka o ličnosti*, „Službeni glasnik RS", br. 97/2008, 104/2009 – dr. Zakon, 68/2012 – odluka US i 107/2012.
28. *Zákoník práce*, No. 262/2006 as amended.
29. *Workplace privacy act 2011*, Australian Capital Territory, Republication No. 3, 2013.

Internet izvori

30. European cort of human rights: Case of Halford v. the United Kingdom, dostupno na: *http://hudoc.echr.coe.int/eng?i=001-58039#{%22itemid%22:[%22001-58039%22]}* (19. 7. 2015).
31. European cort of human rights: Case of Köpke v. Germany, dostupno na: *http://hudoc.echr.coe.int/eng?i=001-58039#{%22itemid%22:[%22001-58039%22]}* (19. 7. 2015).
32. European cort of human rights: Benediktsdóttir v. Iceland, dostupno na: *http://hudoc.echr.coe.int/eng?i=001-93526#{%22itemid%22:[%22001-93526%22]}* (19. 7. 2015).
33. Hendrickx, F.; Protection of workers' personal data in the European Union, dostupno na: *http://ec.europa.eu/social/BlobServlet?docId=2507&langId=en* (13. 6. 2015).
34. The epolicy institute: 2007 Electronic Monitoring & Surveillance Survey, dostupno na: *http://www.epolicyinstitute.com/2007-survey-results* (1. 7. 2015).
35. Privacy protection in the workplace – Guide for employees (Zaštita privatnosti na radnom mestu – vodič za zaposlenike), dostupno na: *http://www.azop.hr/page.aspx?PageID=130* (4. 7. 2015).
36. Shernam, M.; Gov't obtains wide AP phone records in probe, dostupno na: *http://www.ap.org/Content/AP-In-The-News/2013/Govt-obtains-wide-AP-phone-records-in-probe* (3. 7. 2015).
37. Paragraf: Neophodne izmene zakona o zaštiti podataka o ličnosti: nedovoljno regulisane oblasti video-nadzora, biometrijskih podataka, direktnog marketinga i bezbednosnih provera, dostupno na: *http://www.paragraf.rs/dnevne-vesti/270313/270313-vest3.html* (20. 7. 2015).
38. Pravni okvir za primenu video-nadzora, dostupno na: *http://www.parlament.gov.rs/upload/archive/files/lat/doc/istrazivanja/Pravni%20okvir%20za%20primenu%20video%20nadzora%20lat.docx (15. 7. 2015).*
39. Predlog izmena i dopuna zakona o zaštiti podataka o ličnosti (model zakona), dostupno na: *http://www.poverenik.rs/images/stories/model-zakona/modelzzpl.docx* (4. 8. 2015).
40. Wessing, T.; CCTV monitoring in the workplace in Germany, dostupno na: *http://www.taylorwessing.com/globaldatahub/article_cctv_germany.html* (16. 7. 2015).
41. What is closed circuit television (CCTV), dostupno na: *http://whatis.techtarget.com/definition/closed-circuit-television-CCTV* (5. 7. 2015).

MEASURES OF ELECTRONIC MONITORING OF EMPLOYEES AND THE RIGHT TO PRIVACY IN THE WORKPLACE

Ivan Zarkovic
Ministry of Interior of the Republic of Serbia

Summary: At the present time, the development of technology has enabled the application of different systems of monitoring of the workplace, which many employers use as a key to maintain safety and productivity of employees. Regardless of which type of surveillance is on going, employers must take care not to go too far in monitoring, and that they do not violate the rights of employees to privacy. Currently current forms of electronic monitoring of employees, and aims to be achieved by them, evident risks of violations of the rights of employees and their consequences in the field of employment status, as inevitably follows the question of the existence and effectiveness of protection of personal data of employees and their privacy in the workplace. This is seen through the prism of national legislation, and also of the legislation of the European Union. As one of the most common forms of workplace surveillance, video surveillance draws particular attention of the practitioners and theorists. In text, trough analysis of lawful basis and frame of the installation and use of video surveillance equipment, it was point out some contentious issues on this topic. In order to create conditions for a more comprehensive look at the problem and finding adequate solutions in text it was point out at the law of the European Court of Human Rights regarding the application of certain control techniques by the employer and the possible existence of violations of employee rights to privacy.