

Марија Драгићевић,*
Асистент Правног факултета,
Универзитет у Нишу

ОРИГИНАЛНИ НАУЧНИ РАД
doi:10.5937/zrpfni1880421D

UDK: 342.726-057.16

Раđ примљен: 30.09.2018.

Раđ прихваћен: 14.11.2018.

САВРЕМЕНЕ ТЕХНОЛОГИЈЕ И ПРАВО ЗАПОСЛЕНОГ НА ПОШТОВАЊЕ ПРИВАТНОГ ЖИВОТА**

Апстракт: Развој нових информационих технологија довео је до стварања различитих система и алата који омогућавају прислушкивање комуникација, електронски надзор, контролу кретања и одређивање позиција особа, сакупљање података, њихово груписање, претраживање, враћање и реконструкцију, као и коришћење од широког круга корисника. То је омогућило делотворније остваривање послодавчевих овлашћења, али је истовремено створило неслућене могућности за насртаје на приватни живот запосленог. С обзиром на речено, аутор у раду анализира питање допуштености употребе савремених технологија на раду у светлу заштите људских права и основних слобода запослених. Као централни проблем, аутор разматра питање тешкоће довођења у равнотежу интереса послодавца да обезбеди правилно извршавање престације рада и безбедне и здраве услове рада и интереса запослених за поштовањем приватног живота и достојанства на раду. Посебан део рада посвећен је специфичним мерама надзора – контроли употребе службених средстава за комуникацију и видео-надзору.

Кључне речи: приватни живот, приватност, савремене технологије, видео-надзор.

* marijad@prafak.ni.ac.rs

** Раđ је саопштен на међународној научној конференцији „Право пред изазовима савременог доба“, која је одржана 13. и 14. априла 2018. године на Правном факултету Универзитета у Нишу.

Раđ је резултат истраживања на пројекту „Усклађивање права Републике Србије са правом Европске уније“, који финансира Правни факултет Универзитета у Нишу.

1. Увод

Савремене технологије су последица значајног развоја људске мисли и проналазаштва. Појединци, правна лица и државе зависе од њихове употребе јер путем њих обављају или нуде највећи број услуга. Употреба информационаих технологија се последњих година брзо ширила, те није заобишла ни радна места. Поред неспорног доприноса делотворном вршењу послодавчевих овлашћења, развој информационаих технологија је отворио и низ питања која се тичу могућности обезбеђења потребних претпоставки како би легитимни интереси и права субјеката радног односа били адекватно заштићени. Потенцијална опасност од неовлашћеног откривања и злоупотребе података постоји за оба субјекта радноправног односа. Тако, на страни послодавца, постоји бојазан да одређени подаци (нпр. који се односе на поверљиве активности предузећа, финансијске трансакције, управљање кадровима и лични подаци запослених) буду употребљени од стране неовлашћених субјеката, што ствара потребу за инсталирањем уређаја за заштиту и праћење приступа таквим подацима. Поред тога, послодаваци оправдано страхују да ће запослени у току радног времена користити службена средства за комуникацију у приватне сврхе. С друге стране, на страни запослених, главна опасност од употребе савремених технологија лежи у могућности праћења и надзора над извршавањем престације рада, али и одређених аспеката приватног живота, што отвара питање права запосленог на поштовање приватног живота. Полазећи од чињенице да запослени не губе своју приватност тиме што ступају у радни однос, као основно питање у анализи заштите приватног живота запослених намеће се питање обима ограничења права на поштовање приватног живота на раду.

У условима велике несигурности запослења, масовне и дуготрајне незапослености, те ниске стопе синдикализованости, питање остваривања права запослених на поштовање приватног живота у Републици Србији није једно од горућих. Нова и недоречена законска регулатива, те пракса надлежних органа која је тек у повоју условљава потребу ближег и прецизнијег регулисања овог питања аутономним изворима права. У том смислу, рад има за циљ не само да систематизује и критички размотри постојећа решења битна за разумевање права запослених на поштовање приватног живота, већ и да изнесе могуће смернице за његово уређење.

2. Различите концепције „приватног живота“ и „приватности“

Као један од незаменљивих елемената човековог достојанства, право на поштовање приватног живота представља елементарно људско право

загарантовано актима међународноправне природе, уставима већине демократских држава, те инструментима грађанског права. Упркос томе, прецизне дефиниције приватног живота недостају не само правној науци, већ и домаћим изворима права, као и судској пракси. Теорија, законодавство и судска пракса дају различита виђења суштине појма приватног живота и у складу са тим дају и његова различита одређења. Осим несагласности око садржаја самог права, разлике постоје и у погледу терминологије. У упоредном праву се користе различити термини за означавање овог аспекта људског живота: за француско право карактеристична је употреба синтагме „приватни живот“ (*vie privée*), за немачко право израз „приватна сфера“ (*Die Privatsphäre*), у праву држава са англосаксонском правном традицијом најчешће се говори о „приватности“ (*privacy*), док се у праву скандинавских држава, посебно у Шведској, користи реч „интегритет“ (*integritet*) (Hendrickx, 2004: 359).

Тешкоће и разлике у дефинисању приватног живота произилазе, најпре, од тешкоћа у изоловању термина који би био чисто правни, ослобођен од психолошких или социолошких конотација. Други разлог за бројне и различите концепције права на поштовање приватног живота произилазе из чињенице да „приватни живот“ представља један бланкетан појам који се испуњава садржајем тек стављањем у одређени друштвено-историјски контекст (Даниловић, 2017: 163). Међутим, упркос бројним размимоилажењима у виђењу суштине и значења овог појма, међу теоретичарима нема спора да приватни живот означава ограничени простор који није јаван и у којем појединац може независно од спољних утицаја остваривати своје право на слободно обликовање властите личности (Тратар, 2017: 12). У фокусу највећег броја дефиниција приватног живота налази се појам аутономије. Приватни живот се најчешће дефинише као подручје у којем појединац успоставља круг интимног деловања и у којем сме сам одлучивати о томе које ће задирање у њега допустити. У тај простор улазе личне (интимне) ствари које појединац жели задржати заштићене и које према природи ствари или према моралним и другим устаљеним правилима понашања у друштву вреде као такве (здравствено стање, записи, тајни разговори блиских људи итд.) (Тратар, 2017: 12).

Откривању значења гаранције права на поштовање приватног живота у значајној мери су допринела правна схватања Европског суда за људска права у Стразбуру (у наставку Суд), настала у примени чл. 8 Европске конвенције за заштиту људских права и основних слобода, према којем „свако има право на поштовање свог приватног и породичног живота, дома и преписке“.¹ Суд није прецизно дефинисао садржај појма „приватни

1 Европска конвенција дефинише право на приватни живот одвојено од права на поштовање дома и преписке, док се у теорији та права сматрају само делом права на

живот“, имајући у виду његову ширину и често преклапање са другим интересима који уживају заштиту по чл. 8 Конвенције. Уместо нуђења јасне дефиниције, Суд је од случаја до случаја препознавао различите животне аспекте који спадају у оквир приватног живота. Резултат тога је доста магловит појам који суд разуме и тумачи прилично широко (Roagna, 2012: 14). Тако, сходно пракси Суда, концепција приватног живота, између осталог, обухвата следеће области човековог живота: право на успостављање и одржавање односа са другим људима, заштиту физичког и моралног интегритета личности, заштиту личних података, промену личног имена, одређена питања у вези са сексуалном оријентацијом и променом пола (Roagna, 2012: 14–28).

Стављање аутономије у средиште дефиниције приватног живота блиско је значењу који се приписује појму „приватност“ у праву држава са англосаксонском правном традицијом. Иако већина теоретичара не прави разлику између права на поштовање приватног живота и права на приватност, чини се да нема основа за стављање знака једнакости између њих (Упореди: Ковачевић, 2010: 169). Уместо тога, примереније је сматрати их сродним појмовима, будући да, за разлику од (права на) приватни живот које у фокусу има суверену сферу живота појединца (коју чини скуп приватних обележја човека, његових поступака и података о њему) (Ђукић, 2017: 50), (право на) приватност у својој сржи има слободу од контроле или доминације других лица (Ковачевић, 2010: 169). Приватност подразумева право појединца да одлучи које информације о њему могу да се открију другима, као и да одлучи на који начин ће се информације о његовој личности прикупљати и у коју сврху ће се оне користити (Westin, 2003: 433).²

поштовање приватног живота.

2 Везујући се за форму (нарав) државе када је настала, најранија правна анализа концепта приватности, дата у раду «Право на приватност» америчких судија Семјуела Ворена и Луиса Брандајса крајем XIX века, «право приватности» одређује као «право појединца да буде остављен на миру» (Warren, Brandeis: 1890: 195). Ова тзв. класична концепција приватности, иако представља камен темељац теоријском изучавању права на приватност, временом је постала превазиђена. Промењеној нарави државе није више пристајала класична концепција приватности, јер приватни живот појединца у поретку такве државе не може остати сасвим ван захвата државне власти (Прица, 2012: 447, 448). Осим тога, с краја XIX века могући упад у сферу приватности могао је бити учињен само на пасивном субјекту, који је жртва злоупотребе одређених техничких изума, чије примене често није свестан или их није желео (Даниловић, 2017: 164). Временом је то престало бити случај. Развој и употреба информационо-комуникационе технологије и електронске комуникације је створила неограничене могућности за концентрацију података, њихово груписање и претраживање по разним обележјима, као и могућност коришћења од стране широког круга корисника. Зато се појављују

У теорији (нарочито англосаксонској) разликују се три врсте приватности: просторна, комуникациона и информациона. **Просторном приватношћу** појединац се штити од упада у интимну сферу тамо где очекује да ће бити сам. Његов дом (стан) је прво, али не и једино такво место. Заштићен је и на сваком другом месту где може основано и тиме очигледно за друге очекивати да неће бити изложен очима јавности, макар да се ради само о столу на радном месту (Тратар, 2017: 12; Бобан: 2012: 584, 585). Код *комуникационе приватности*, пак, предмет заштите је слободна и ненадзирана комуникација. Овим аспектом приватности штити се интерес појединца да се држава или непозване треће особе не упознају са садржајем поруке коју то лице посредује преко било којег средства комуникације, као и интерес појединца да има надзор над тиме коме, у каквом опсегу, на какав начин и под каквим ће условима посредовати одређену поруку. Комуникациона приватност се не може сузити на садржај извештавања, већ обухвата податке о томе на који се начин одвијала, ко је успоставио, с ким је била успостављена, одакле је успостављена и да ли се уопште одвијала (Тратар, 2017: 13). *Информациона приватност* подразумева да појединац одлучује коме ће, када и колико саопштити личне податке, водећи рачуна о својим правима и потребама заједнице. У америчкој правној литератури могуће је уочити неколико концепција информационе приватности. *Прву концепцију* чини информациона приватност као ненаметање. Према овој концепцији „информациона приватност подразумева немешање у личне ствари“ (Miller, Weckert, 2000: 256). Другим речима, појединци имају право да не буду предмет уплитања других лица у односу на одређене информације. Ова дефиниција веома зависи од културолошког окружења и скреће фокус са процеса приватности, јер би одређене форме информација требало третирати као приватне, нпр. личне односе, чињенице о личним изборима (као што је гласање), као и податке о томе шта појединац има у свом власништву (Miller, Weckert, 2000: 255–265). *Другу концепцију* представља информациона приватност као процес одвајања и избегавања. Тако, на пример, Jourard сматра да је приватност стање које се постиже задржавањем информација о понашању појединца у прошлости, као и о намерама које појединац има везано за будућност (Jourard, 1966: 307–318). Pedersen, пак, сматра

нове, савремене, концепције приватности које посматрају приватност као активну, а не пасивну вредност - као право на контролу информација о свом животу, а не само као забрану од упада других у приватни живот. Приватност појединца се сада посматра као право појединца да сам одреди када, како и у којој мери ће информације о себи саопштавати другим лицима. Он има право да контролише ко користи информације о њему, када, у које сврхе, да ли има овлашћења за то, да ли је дошло до промена тих информација, зашто итд. (Димитријевић, 2011: 203, 204).

да се приватност информација састоји од шест димензија: (а) изолација, (б) самоћа, (ц) блискост са пријатељима, (д) присност са породицом, (е) резервисаност, и (ф) анонимност. Све ове димензије указују на то да се приватност постиже сепарацијом и повлачењем из спољног света (Pedersen, 1997: 147–156).³ Најзад, *према трећој концепцији*, информациона приватност се одређују као „жеља појединаца, група или институција да одреде себе у смислу када, како и до ког степена се информације о њима преносе другим лицима“ (Westin, 1967: 166–170). По овим концептима, приватност је процес који подразумева контролу граница приватности, при чему појединац контролише ко има, а ко нема приступ њему самом (Snyder, 2010: 271).⁴

3. Право запослених на поштовање приватног живота

Концепција права на поштовање приватног живота се мења не само у времену, већ и у простору. Тако, док се у САД полази од права власништва над средствима за рад које послодавцима даје право да контролишу

3 Дефиниције које су базиране на концептима „ненаметања“ и „сепарације и избегавања“ су сличне у том смислу да подржавају теорију да се приватност постиже на тај начин што се друга лица удаљавају од себе. По овим дефиницијама, приватност је стање које се може постићи када појединац може да спречи друге да се мешају у његов живот, када се може да сакрије информације од других, или када може бити изолован од других. Такође, ове дефиниције указују на то да појединац може достићи идеално стање приватности, те да су неке информације приватне без обзира на њихов садржај. Једно од ограничења ових дефиниција је да не успевају да покрију динамичну природу приватности, већ само њен оквир који је веома статичан (Snyder, 2010, 270).

4 У литератури се у прилог треће концепције информационе приватности наводе емпиријски подаци. Примера ради, *Fusilier* и *Hoyer* су разматрали да ли студенти дозвољавају приступ информацијама које се налазе у њиховом личном досијеу (ово се односи на личне информације и на информације које се односе на пословни учинак) и откривање таквих информација трећим лицима која су повезана са послом који траже. Само они појединци којима је дата контрола над начином на који су њихове информације коришћене изјавили су да осећају да је приватност њихових информација испоштована (Fusilier, Hoyer, 1980: 623–626). *Tolchinsky* је са групом истраживача открио да, уколико запослени не могу да контролишу начин на који компанија користи њихове личне информације, они аутоматски осећају да је њихова приватност угрожена (Tolchinsky, McCuddy, Adams, Ganster, Woodman, Fromkin, 1981: 308–313). Преиспитивање приватности из угла контроле превазилази ограничења које имају дефиниције базиране на концепту „ненаметања“ и „сепарације и избегавања“. Важно је нагласити да је концепт контроле укључен у све претходне дефиниције. На пример, гледајући из перспективе контроле, појединац може остварити приватност у интимној вези тако што задржава одређене информације за себе или тражи самоћу. Међутим, дефиниција је знатно шира јер појединац може изабрати да подели личне информације са другим лицима и опет осећати да му приватност није угрожена (Snyder, 2010: 271).

њихову употребу и понашање запослених (Miller, Wells: 2007: 323)⁵, у европској пракси се полази од дијаметрално супротног приступа – од идеје приватности као основног људског права, гарантованог и заштићеног међународним конвенцијама⁶ и националним законодавствима⁷ (Даниловић, 2017: 173). Оваквом разумевању гаранције права на поштовање приватног живота, значајно је допринела јуриспруденција Европског суда за људска права у којој је изграђен став да се поштовање приватног живота протеже и на “професионалне или пословне активности”. Према ставу Суда не постоји начелан разлог зашто би појам “приватног живота” требало да искључи стручне и пословне активности, будући да се односи са

5 Тако, на пример, у предмету Smyth (1996) Суд је сматрао да не постоји разумно очекивање приватности у електронској комуникацији коју запослени вољно чини преко електронске поште послодавца, без обзира на то да ли се врши пресретање комуникације од стране послодавца. Према ставу Суда, иако запослени имају валидан интерес у смислу приватности своје електронске комуникације, интерес послодавца у смислу спречавања неодговарајућих и непрофесионалних коментара и нелегалних активности преко електронске поште компаније има већи значај (Friedman, Reed, 2007: 79). Штавише, у погледу права послодавца да контролише компјутерску опрему коју је дао на располагање запосленима, Седми Апелациони суд сматра „да је злоупотреба приступа компјутерима на радном месту толико уобичајена (имајући у виду да их запослени врло често користе као медијум за оговарање и забаву, чиме се омета процес рада), да се недостатак контроле истих може сматрати и неодговорношћу послодавца“ (Friedman, Reed, 2007: 79).

6 Одговарајуће гаранције права на поштовање приватног живота садржане су у: чл. 12 Универзалне декларације о људским правима; чл. 17 Међународног пакта о грађанским и политичким правима; чл. 8 Европске конвенције за заштиту људских права и основних слобода; чл. 7 Повеље Европске уније о основним правима. Лични подаци, као део права на поштовање приватног живота, заштићени су и: Смерницама ОЕЦД за заштиту приватности и прекогранични ток личних података; Кодексом праксе МОР о заштити личних података радника; Конвенцијом СЕ о заштити лица у односу на аутоматску обраду личних података из 1981. године; Директивом бр. 95/46 о заштити лица у погледу коришћења њихових личних података и о слободном кретању таквих података – која је престала да важи 25. маја 2018. године, даном почетком примене Опште уредбе о заштити података о личности (ЕУ 2016/679); Директивом бр. 2002/58 о коришћењу личних података и заштити приватности у сектору електронских комуникација и бројним другим актима (Јашаревић, 2016: 71–92).

7 Правна форма признавања овог права разликује се, те поједине државе изричитим уставним одредбама установљавају право на приватност (пример Белгије, Шпаније, Португалије), док друге право на приватност изводе из националне судске праксе или прихваћених међународних обавеза (Аустрија, Данска, Француска, Италија) (Hendriks, 2002). У Републици Србији се уставним одредбама признаје заштита података о личности (чл. 42), док се Законом о раду из 2005. године у радно законодавство први пут уводи институт заштите личних података, али се то право уређује само у два члана (чл. 83 и индиректно чл. 26). Остала питања у овој области регулише Закон о заштити података о личности из 2008. године.

другим људима управо најчешће успостављају и развијају током обављања професионалних активности. Поступајући у случају Нимиц против Немачке, Суд је заузео став да би било сувише рестриктивно ограничити појам приватног живота на “унутрашњи круг” у коме појединац можда проводи свој лични живот по сопственој жељи, а из њега потпуно искључити спољашњи свет који се налази унутар тог круга. Ускраћивање заштите чл. 8 Конвенције из разлога што се оспорена мера односи само на пословну активност би могло да доведе до неједнакости у поступању према људима, због тога што би таква заштита остала да постоји за оне код којих није могуће разликовати пословне од непословних активности. Суд је своје мишљење поткрепио и чињеницом да је у одређеним државама уговорницама за реч “дом” прихваћено да обухвата и пословне просторије, које тумачење је у складу са француским текстом чл. 8 Конвенције (“*domicile*”).⁸

Концепт права на поштовање приватног живота нејасан је и дискутабилан сам по себи. Уколико га посматрамо у оквирима радног односа он постаје још неухватљивији, имајући у виду да радни однос установљава субординацију запосленог, због чега и идеја приватности трпи одређене модификације (Даниловић, 2017: 178, 163). Разматрање субординације у радном односу рађа питање утврђивања граница послодавчеве (управљачке, нормативне и дисциплинске) власти, те разграничења приватног и професионалног живота запосленог. У анализи наведеног питања Љубинка Ковачевић полази од месног и временског критеријума⁹ наводећи да је подручје послодавчеве власти (и правне субординације у радном односу) ограничено на радно време и место рада. Изван радног времена и места рада послодавчева власт, у начелу, не допире до запосленог и сфере његове аутономије, која се означава термином „приватни живот“. Приватни живот, стога, представља простор у којем запослени има потпуну слободу да одлучује о својим активностима и из којег може да искључи друга лица (Ковачевић, 2010: 168, 169). Концентрисање дефиниције приватног живота око појма аутономије, међутим, никако не подразумева да се професионални живот и аутономија међусобно искључују, већ значи да радни однос нужно подразумева умањење (не и укидање) аутономије

8 Пресуда Европског суда за људска права у случају *Niemietz v. Germany* од 16. децембра 1992 (представка 13710/88).

9 Ковачевић наглашава да, упркос томе што радно време и место рада *a priori* представљају објективне и једноставне критеријуме, исти не омогућавају повлачење јасне границе између подручја професионалног и приватног живота, те их треба користити опрезно. Када је у питању месни критеријум, на опрез највише позивају случајеви у којима запослени обављају послове ван просторија послодавца, док на непоузданост временског критеријума указују случајеви као што је приправност за рад. Видети више: (Ковачевић, 2013: 491; Ковачевић, 2010: 168).

запосленог на месту рада у мери у којој је то неопходно за конкретно извршење престације рада (Ковачевић, 2013: 489). У том смислу, могуће је приметити да се аутономија запосленог на радном месту ограничава, преваходно, због потребе правилног извршења престације рада. Зато и није могуће сачинити неки исцрпан списак допуштених ограничења аутономије запосленог на раду будући да различите ситуације, различите врсте послова и радних места повлаче са собом другачија очекивања у смислу приватности, као и другачије начине заштите.

4. Допуштеноост ограничења права запослених на поштовање приватног живота

Интересу послодавца да спречи ненаменско коришћење средстава и обезбеди сигурност радног места, тј. да користи своја управљачка, нормативна и дисциплинска овлашћења супротставља се интерес запослених да заштите своју приватну сферу. Ову супротстављеност додатно појачава брз и интензиван технолошки развој, који је послодавцима омогућио да у вршењу својих овлашћења користе технологије за пренос и обраду података, укључујући електронски и видео-надзор. Регулисање употребе савремене информационе технологије на радном месту у циљу контролисања правилног извршавања престације рада је велики изазов за законодавце. Упркос утицају судске праксе, научних посленика, органа за заштиту личних података и других државних органа, још увек нема убедљивих, прецизних и заједничких правних одговора. Аналогија са другим институтима може помоћи, али може бити и погрешна када се ради о технолошки иновативним феноменима, посебно када је у питању регулисана понашања везаних за интернет. Правни прописи би, стога, као приоритет, требало да утврде опште принципе, инспирисане рационалношћу и праведношћу, а не да утврђују детаљна правила која услед интензивног технолошког развоја брзо застаревају. Овакав поступак захтева претходну идентификацију интереса обе стране (послодаваца и запослених) и узимање у обзир њихова међусобна права, обавезе и одговорности, како би се правилно уравнотежила супротна очекивања (Lugaresi, 2010: 163).

4.1. Контрола употребе службених средстава за комуникацију

Обезбеђивање од стране послодавца средстава за рад, укључујући и компјутерске системе који имају приступ интернету, носи са собом проблематику регулисања права послодавца да прати и контролише учинак запосленог и начин на који их запослени употребљава. Посматрано

из угла запосленог, основна средства за рад која послодавац обезбеди се морају користити за извршавање задатака и обављање пословних дужности (Georghe, 2017: 62). Будући да је намена службених средстава за комуникацију у потпуности везана за извршавање престације рада, послодавац, као њихов власник, има право да контролише и ограничи употребу ових средстава. Та врста контроле отвара низ спорних питања, од којих су посебно деликатна два: прво је да ли запослени имају право на коришћење службених средстава за комуникацију у личне сврхе а, ако имају, у којој мери; а друго је могу ли послодавци легитимно пратити (контролисати) понашање запослених коришћењем савремених технологија и, ако могу, у којој мери, под којим условима и у које сврхе.

4.1.1. Употреба службених средстава за комуникацију у приватне сврхе

Иако је употреба службених средстава за комуникацију везана за извршавање престације рада, у литератури постоји готово опште схватање да коришћење службених средстава у приватне сврхе треба дозволити или бар толерисати, посебно када је реч о приступу интернету и слању и пријему електронске поште преко службеног рачунара. Забрана употребе интернета у личне сврхе од стране запослених се у литератури сматра непрактичном и помало нереалном, јер не уважава степен до којег интернет може помоћи запосленима не само у њиховом свакодневном информисању и изражавању, већ и у сарадњи са другима и пословању (Lugaresi, 2010: 163). Поред тога, ваља указати и на тешкоће надзора у случају употребе службених средстава за комуникацију у личне сврхе, што је више правна (тешко је дефинисати сва понашања и поставити границе између законите и незаконите активности) од техничке непрактичности (праћење интернета на радном месту технички може бити прилично лако). Парадоксално, али ако би се забрана личне употребе средстава за комуникацију сматрала немогућом, постојале би две алтернативе: 1) забранити надзор, индиректно потврђујући право на личну употребу, или 2) омогућити надзор послодаваца, како би се смањиле злоупотребе. Прихватањем прве опције запослени би могли имати приступ интернету онако како (и у обиму у којем) желе, спречавајући послодавце да ефикасно воде своје пословање. У случају прихватања друге опције, пак, послодавци би имали право да контролишу употребу средстава за комуникацију од стране сваког запосленог. Проблем који се у овом случају јавља јесте постављање границе приступа овим средствима. Тако, на пример, ограничен приступ интернету, даје право послодавцу да проверава којим веб страницама је запослени приступио (како би утврдио да ли су у питању „легитимне“ веб странице), те колико времена је проведено на њима (да

би утврдио да ли је прекомерно). „Зонирање“ веб страница на „радно-везане“, „дозвољене“, „толерисане“ и „забрањене“, међутим, није нимало лак задатак (Lugaresi, 2010: 165). Због тога, препорука већине аутора који се баве овом проблематиком јесте доношење од стране послодавца интерне регулативе којом се јасно регулише питање коришћења од стране запослених средстава рада и опреме у приватне сврхе, те им се наглашава да (ли) могу бити предмет контроле (привремене или трајне) која се односи на начин коришћења средстава за рад (Halcrow, 2002: 46–48).

Уколико је употреба службених средстава за комуникацију за личне потребе регулисана, политика заштите података послодавца би требало да понуди разјашњења у смислу метода, услова и ограничења. Регулисање наведених питања појединачним уговором о раду, у којем се дефинише да запослени може бити предмет контроле, није само по себи довољно, већ је потребно сачинити засебан писани документ у којем ће се јасно дефинисати начин контроле (уколико се прати ток разговора или његов садржај), њено трајање и сврха, као и могуће последице. У правилнику о приватности је, најпре, неопходно регулисати да ли је коришћење интернета за личне потребе дозвољено или не, јер степен надзора зависи искључиво од ове ставке. Уколико употреба интернета за личне потребе није дозвољена, одређена правила (нпр. забрана скидања музичких фајлова или коришћење веб-мејла) могу бити сувишна. Уколико је дозвољено коришћење интернета за личне потребе, степен контроле би требало да дефинише питање деликатних и поверљивих информација.

У недостатку регулативе и изричите забране сматра се да је употреба службених средстава за комуникацију у приватне сврхе допуштена. Претпостављена дозвола подразумева и разумну употребу рачунара за личне потребе, која значајније не омета запосленог у извршавању послова и није усмерена на остваривање лукративног циља“ (Ковачевић, 2013: 517).

4.1.2. Право послодавца да контролише употребу службених средстава за комуникацију

Друго значајно питање у вези са службеним средствима за комуникацију је да ли послодавац може легално контролисати њихово коришћење и, уколико може, до ког степена то може чинити, под којим условима и са каквим последицама. Суштина овог питања тиче се, заправо, решавања сукоба одговарајућих послодавчевих овлашћења са правом запослених на поштовање приватног живота.

У складу са чл. 8 Конвенције, саставни део права на поштовање приватног живота чини право на поштовање преписке. Циљ права на поштовање

преписке је заштита тајности приватних комуникација грађана, и оно је у пракси Европског суда за људска права тумачено тако да гарантује право на непрекидну и нецензурисану комуникацију с другим лицима. „Праг заштите је висок, будући да не постоји никакво *de minimis* начело да би дошло до ометања: отварање једног писма је довољно“ (Roagna, 2012: 33). Суд је редовно узимао у обзир технолошки непредак у области комуникација, и усвојио развојно тумачење речи „преписка“. Поред класичне преписке на хартији, за сврху чл. 8 Конвенције, „преписком“ се сматрају и: старији облици електронске комуникације, као што су телекси; телефонски разговори, укључујући информације које се односе на њих, као што су датум, трајање и бројеви који су бирани; поруке на хартији; електронске поруке (и-мејлови), као и подаци који потичу из праћења личног коришћења интернета; приватне радијске комуникације, али не када су обављене на јавним таласним дужинама па друга лица могу да им приступају; преписка пресретнута током пословних активности или из пословних просторија; електронски подаци одузети током претраге адвокатске канцеларије; пакети одузети од стране царинске претраге. Према ставу Суда, садржај преписке није од значаја за питање ометања: оно што штити чл. 8 је средство или метод, а не предмет комуникације (Roagna, 2012: 33).

Право на поштовање преписке остварује се и на раду, и то, у погледу различитих облика комуникације запосленог са трећим лицима. У погледу приступа интернету и слања/пријема електронске поште, питање права на поштовање приватног живота се, у првом реду, поставља у вези са условима коришћења компјутерских алата од стране запослених, као и правом послодавца да врши надзор над онлајн активностима запослених. Реч је, прецизније, о могућности контролисања од стране послодавца односа веб страница – време, те садржаја страница којима запослени у току радног времена приступају. У вези са наведеним, у јуриспруденцији Европског суда за људска права заузет је став да је послодавчев надзор над употребом службених средстава за комуникацију допуштен само ако је претходно испуњено неколико услова.¹⁰

10 Недавно је Европски суд за људска права у предмету Барбулеску против Румуније пресудио да национални судови нису осигурали поштовање права на приватност у ситуацији када је запослени дисциплински кажњен отказом од стране послодавца због коришћења интернета и електронске апликације у приватне сврхе током радног времена. Иако постоје одређене контроверзе у вези пресуде, она је временом постала одличан, чак визионарски, пример права на поштовање приватног живота на раду и начина контролисања активности запослених од стране послодавца. У овом случају запослени је, на захтев послодавца, користио апликацију *Yahoo Messenger* за комуникацију са клијентима. Послодавац је, без знања запосленог, вршио надзор над

Први услов допуштености послодавчеве контроле јесте његова обавеза да запослене *уозна* са могућношћу контроле. Одлука о контроли се мора донети пре почетка процедуре праћења активности запослених, а запослени (без обзира на то што је одлука о контроли донета једнострано) мора бити обавештен о почетку контроле пре њеног отпочињања. У одлуци о увођењу контроле послодавац мора навести начин на који ће

коришћењем те апликације и утврдио да је запослени исту користио и за приватну комуникацију, због чега је добио отказ. Национални судови су сматрали да је одлука о отказу донета у складу са законом, након спроведеног дисциплинског (истражног) поступка у којем се показало да је запослени прекршио одредбе унутрашњег прописа за које је знао и којим је била предвиђена забрана коришћења ресурса послодавца у приватне сврхе. Национални судови су сматрали да је мера коју је послодавац предузео била легитимна и пропорционална циљу, те да је у овом случају постигнут потребан баланс између права послодавца да надгледа рад запослених и права запослених на поштовање приватног живота. У првом степену, Европски суд за људска права је подржао одлуку националних судова и утврдио да овде нема кршења приватности, наводећи да је у конкретном случају истрага послодавца била ограничена у обиму – искључиво се односила на апликацију и пропорционална – узимајући у обзир интерес послодавца да потврди да запослени обавља послове свог радног места у радно време. Према томе, Суд је потврдио да је држава Румунија предузела неопходне мере како би осигурала поштовање права на приватни живот и тајност кореспонденције, те да није било кршења чл. 8 Конвенције. Међутим, дана 6. јуна 2016. године, на захтев подносиоца жалбе, предмет је упућен Великом већу Суда, које је, анализирајући случај, дана 5. септембра 2017. године, пресудило да национални судови нису осигурали поштовање права на приватност запосленог који је дисциплински кажњен отказом због коришћења интернета и ИТ апликације у личном интересу током радног времена, при чему је послодавац своју одлуку заснивао на доказима добијеним надгледањем електронске комуникације запосленог, без његовог знања. Суд је закључио да национални судови нису успели успоставити потребан баланс између права запосленог на поштовање приватног живота и права послодавца да надгледа и контролише рад својих запослених. Стога је Суд утврдио кршење чл. 8 Европске конвенције о људским правима. У својој одлуци, Суд је одредио критеријуме које ће националне власти применити у циљу постизања равнотеже између права двеју странака (послодавца и запослених): да ли је запослени обавештен о томе да послодавац има могућност праћења електронске поште и других средстава комуникације (обавештење мора јасно означавати природу мониторинга); степен контроле и степен мешања у приватни живот запосленог (у том случају је потребно направити јасну разлику између контролисања тока разговора и садржаја разговора); да ли послодавац има адекватне разлоге да оправда контролу и да ли има приступ садржају разговора; да ли послодавац може користити мере и методе који се мање мешају у приватне ствари запослених лица; да ли је контролисање запослених неопходно за остваривање циља који је поставио послодавац; да ли је запослени заштићен адекватним мерама, посебно уколико се послодавац контролом меша у приватни живот запосленог. Суд сматра да се радни однос мора заснивати на међусобном поверењу послодавца и запосленог лица. Видети: Пресуда Европског суда за људска права у случају *Bărbulescu v. România* од 5. септембра 2017. године (представка 61496/08).

контрола бити реализована и разлоге због којих је неопходна. Запослени се не мора сложити са начином обављања контроле, али сакупљање и чување личних података који су прикупљени у поступку контроле захтева његову сагласност. Уколико послодавац није изричито навео да је праћење активности на интернету и кореспонденције електронском поштом могуће, запослени претпостављају да до контроле неће доћи. Њихова очекивања заснована су на концепту „разумно очекиване приватности“.¹¹ Примена овог концепта значи да је послодавцу забрањено да врши надзор и да се меша у комуникацију запосленог, ако запослени, имајући у виду све околности конкретног случаја, није могао да очекује да послодавац надзире његову преписку или разговор.¹²

Поред тога што послодавчева контрола мора бити транспарентна, да би била допуштена, она мора бити и *оправдана*. Она се, у том смислу, мора заснивати на законитим интересима. Тако, сасвим је оправдано да послодавац контролише трошкове које праве запослени, као што је оправдано да контролише запослене ради спречавања незаконитих поступања. Као легитимни интерес увођења контроле може се јавити и идентификација компјутерских вируса, елиминисање преоптерећености мреже, контролисање начина обављања задатака, идентификација кршења обавезе поштовања клаузуле забране конкурентности, као и провера поштовања репутације послодавца.¹³

11 Концепт разумно очекиване приватности је развијен у америчкој судској пракси, тумачењем IV амандмана Устава САД, којим се штити неповредивост дома, докумената и имовине америчких грађана. Бавећи се питањем неовлашћеног прислушкивања грађана у контексту тог амандмана, судови САД су средином XX века формулисали правило да се приватност појединца може заштити ако је појединац испољио стварно очекивање приватности и ако је његово очекивање такво да је друштво спремно да га призна као „разумно“. Примена овог правног стандарда је временом проширена и на односе запослених и послодавца, без већих измена (Даниловић, 2017: 172).

12 Концепција разумно очекиване приватности је у пракси Европског суда за људска права први пут поменута у случају Халфорд против Велике Британије од 25. јуна 1997. године. У овом случају послодавац је, без знања запослене, прислушкивао њене телефонске разговоре на радном месту. Одбрана је тврдила да запослена није могла имати разумно очекивање приватности у погледу коришћења телефона на радном месту и да је послодавац принципијелно слободан да без знања запосленог надзире телефонске разговоре у случају када запослени користи службене телефоне. Међутим, Суд је пресудом утврдио да „упад“ послодавца у разговоре представља повреду гаранције права на поштовање приватног живота, зато што запослена није била упозорена на послодавчеву могућност мешања у телефонске разговоре који се воде из послодавчевих просторија. Видети: Пресуда Европског суда за људска права у случају *Halford v. the United Kingdom* од 25. јуна 1997. године (представка 20605/92).

13 Имајући у виду да право послодавца да контролише приступ интернету и електронску пошту запосленог у свим горе наведеним ситуацијама може нарушити

Последња група услова везана за допуштеност послодавчеве контроле тиче се њене *примерености и нужности*, због чега је, у начелу, забрањена константна и систематска контрола употребе службених средстава за комуникацију, а иста може бити примењена само у случају када послодавац закониту сврху надзора није могао остварити мерама и методама које представљају мањи упад у приватне ствари запослених. Осим тога, послодавац треба да надгледа комуникацију запослених на начин који је, у техничком смислу, примерен, те да приликом надзора прикупља само одређене врсте података, и то оне који су непосредно везани за извршавање обавезе рада. (Ковачевић, 2013:520-521). Податке прикупљене током контроле послодавци могу користити само у складу са легитимним интересима, те их, стога, морају уништити у тренутку када више нису неопходни. У том смислу, заштити послодавчевих интереса више доприноси спречавање, него откривање, ненаменске употребе интернета, а тај вид контроле уједно представља и мањи упад у интимну сферу запосленог. У такве мере се, на пример, могу сврстати подешавање рачунара тако да запослени не могу визуелно сакрити своје електронске активности (мања је вероватноћа да ће запослени користити интернет знајући да њихове колеге, клијенти и остали могу видети оно што имају на монитору рачунара), технолошке мере, као што су филтери који забрањују одређене операције или приступ одређеним сајтовима и сл.¹⁴

4.1.3. Надзор електронске поште запосленог

Најделикатније питање у вези са контролом употребе службених средстава за комуникацију јесте праћење електронске поште, имајући у виду могућност сазнавања садржаја преписке што представља најдубље задирање у интимну сферу. У циљу утврђивања постојања права послодавца да врши надзор електронске поште, у теорији (пре свега америчкој) пошло се од права власништва. Према једној групи теоретичара, уколико запослени користе компјутере и мрежу за електронску пошту у власништву послодавца, не могу очекивати потпуну приватност, јер послодавац може проверити сваки компјутер, мрежу и прочитати садржај сваке примљене

баланс између права запослених на поштовање приватног живота и његових одговарајућих овлашћења, легитимни интереси (оправдани разлози) увођења надзора се не могу дефинисати генерално, већ само од случаја до случаја.

14 Поузданост белих и црних листа веб-сајтова је, међутим, веома мала, имајући у виду да се нови веб-сајтови и странице креирају на дневном нивоу. Активност ажурирања филтера уопште није лака, а црне листе забрањених веб-сајтова се стално умножавају и генеришу нове веб-сајтове који нису предмет филтрирања, док беле листе дозвољених сајтова константно блокирају нове сајтове који могу бити корисни (Lugaresi, 2010: 172).

и послате електронске поруке. Запослени не могу имати иста очекивања везана за приватност на радном месту у поређењу са очекивањима везаним за приватност коју имају код куће. Према присталицама другог схватања, пак, власништво над мрежом која покрива електронску пошту не подразумева власништво над електронском поштом. Електронска пошта је „затворена“ кореспонденција и мора законски бити третирана као таква. Чињеница да послодавци поседују адресе електронске поште не значи да поседују њихову електронску пошту, још мање да имају право да је читају. Ово не значи да послодавац не може вршити надзор електронске поште запослених. Интерна политика заштите податка може навести да није дозвољено слање и примање личне електронске поште на радном месту, те да је електронска пошта „изједначена“ са факсом (и да се може читати и архивирати од стране послодавца). Очекивања од приватности се у том случају знатно мењају, штавише нестају. У свим другим случајевима, контрола садржаја електронске поште не би се могла сматрати допуштеном.¹⁵

4.2. Видео-надзор у радном простору

Употреба различитих техничких средстава за контролу кретања и одређивања присуства запослених у просторијама послодавца, попут идентификационих картица, инсталације камера и увођења биометријских система, који омогућавају препознавање запослених на основу неког непроменљивог физичког својства (нпр. узимањем отиска палца или снимањем зенице), може допринети ефикаснијем вршењу послодавчевих овлашћења (Ковачевић, 2013: 524). Инсталација система видео-надзора, тако, може представљати вид заштите од разних прекршајних и криминалних радњи запослених и других лица, меру заштите запослених и имовине, средство унапређења продуктивности (контрола обављања посла и техничких средстава), а може се користити и као доказ у случају спора између послодавца и запосленог (Жарковић, 2015: 171). Међутим, коришћење система оптичке контроле и надзирања запослених путем камера, изазвала је жучне научне и стручне расправе, које су, потпуно оправдано, биле усмерене на питање допуштености примене ове надзорне мере, посебно ако се има у виду да иста укључује снимање радњи и гестова запослених (Ковачевић, 2013: 525). Као препреке у примени система видео-надзора пословног простора наводе се психолошки притисак на запослене,

15 За разлику од службених мејлова чији надзор послодавци могу спроводити, уз поштовање правила дефинисаних интерним актима, отварање приватних мејлова (који су као такви означени) је апсолутно забрањено, и то независно од тога да ли је послодавац претходно забранио употребу службених рачунара у приватне сврхе.

могућност злоупотребе снимљеног материјала, задирање у приватност запослених и нарушавање њиховог достојанства.

У државама чланицама Европске уније урађена је студија под називом „Заштита личних података запослених: случај надзора и праћења“, финансирана од стране Европске комисије и Генералног директората за запошљавање и социјална питања. У Извештају студије, по питању надзора и праћења запослених, наведено је да употребу камера у радном окружењу треба сматрати законитом уколико се надзор примењује ради заштите здравља и безбедности, заштите имовине послодавца, праћење процеса производње и праћења радног учинка. Праћење не би требало да буде трајно, не би се смело вршити у приватним областима, а тајни надзор је дозвољен у веома ограниченим случајевима (нпр. уколико постоје основи сумње да је узвршено кривично дело).¹⁶

У литератури, националним законодавствима¹⁷, али и пракси Европског суда за људска права¹⁸ искристализована су основна начела допуштености

16 Наведено према: Жарковић, 2015: 172.

17 У већини држава чланица Европске уније, али и државама региона, коришћење видео-надзора на радном месту, по правилу, није непосредно регулисано законом, већ се заштита запослених од недопуштене употребе видео-надзора обезбеђује на основу норми (уставног, управног, кривичног, радног права) које гарантују заштиту достојанства и поштовање приватног живота (Ковачевић, 2013: 528). Има држава, попут Белгије, у којима се ово питање регулише колективним уговорима и једностраним актима послодавца (De Hert, Loncke, 2005: 167–205). Најчешће се, међутим, контрола понашања запослених од стране послодавца регулише законима о заштити личних података, имајући у виду да видео-надзор заправо представља сакупљање података о личности.

18 Тако, на пример, у случају Копке против Немачке од 5. октобра 2010. године подносилац представке била је радница, благајник у супермаркету, која је отпуштена због наводне крађе, при чему је као доказ послодавац приложио снимак са видео-надзора који је прибављен уз помоћ детективске агенције. Видео-надзор подносиоца представке је спроведен без претходног упозорења од стране послодавца. Снимци који су на тај начин добијени прегледани су од стране неколико запослених и коришћени су касније у судским поступцима у земљи. На овај начин снимци су постали доступни јавности, а подносилац представке позвала се на повреду чл. 8 Конвенције. С друге стране, послодавац је истицао да су предузете мере биле временски ограничене на две недеље, да је снимано само подручје где је запослена радила, а да су добијени подаци коришћени само од стране ограниченог броја лица која су запослена код истог послодавца и све искључиво ради доказивања незаконитог понашања запослене. Суд је закључио да у овом случају не постоји ништа што би указивало на то да су домаћи органи пропустили да заштите правичну равнотежу између права запослене на поштовање приватног живота и интереса послодавца у заштити имовинских интереса. Образлажући пресуду, Суд је навео да је у конкретном случају тајни надзор спроведен тек након што је послодавац приметити неправилности на рачунима, да

примене система видео-надзора у просторијама послодавца: 1) *Начело законитости* подразумева да се свака обрада личних података мора обављати на законит начин, уз поштовање достојанства и приватности запослених; 2) *Начело оправданости* подразумева да послодавац може користити камере и надзор у радним просторијама само онда када је снимање места рада нужно за заштиту његових легитимних интереса, пре свега његове потребе да обезбеди личну сигурност запослених и других лица у просторијама, да заштити имовину или надзире исправност производних процеса, као и ради спречавања (или истраге) ситуација којима се угрожавају безбедност имовине или производни процеси, ако је то једини могући начин контроле; 3) *Начело транспарентности* подразумева да запослени морају унапред бити обавештени о примени ове мере, о њеним циљевима, о броју инсталираних камера, о месту њиховог постављања, трајању снимања, евентуалном (привременом) чувању података, као и о контакт особи која рукује прикупљеним подацима. То, даље, значи да је забрањен тајни видео-надзор, осим у изузетним случајевима када постоји основана сумња о криминалној активности или другом озбиљном незаконитом поступању.¹⁹ 3) *Начело сразмерности* подразумева да лични подаци који се обрађују морају бити релевантни с обзиром на сврху обраде. Примена видео-надзора мора бити ограничена на радно време и место рада. У свакој просторији која се снима мора постојати слика камере, а видео-надзор се не сме уводити у тоалетима, свлачионицама, соларијумима, ресторанима односно свуда где се драстично задира у приватност особа. Постављање камера у наведеним тзв. полуприватним просторијама се сматра неоправданим и, последично, недопуштеним, чак и ако постоје озбиљни разлози за њихово инсталирање. Уз то, камера не сме бити постављена тако да снима само једног запосленог. Са друге стране, временско ограничење видео-

је био ограничен временски и просторно, те да је послужило и као средство да се са осталих запослених скине сумња. На крају, Суд је констатовао да није био ниједног другог једнако ефикасног средства за заштиту имовинских интереса послодавца којим би се у мањој мери задирало у приватну сферу подносиоца представке. Видети: Пресуда Европског суда за људска права у случају *Köpke v. Germany* од 5. октобра 2010. године (представка 420/07).

19 Према мишљењу Савезног радног суда Немачке, тајни видео-надзор запосленог дозвољен је: уколико се сумња на кривично дело или друго масовно кршење прописа од стране запосленог на штету послодавца, уколико све блаже методе истраживања нису дале резултате, уколико је тајни видео-надзор једино решење да се проблем реши и уколико примена није несразмерна. У таквим случајевима, надзор мора да се концентрише на запосленог за кога се претпоставља да крши прописе или чини кривично дело и на места где се очекује да се кривично дело или друго кршење прописа дешава (на пример каса) (Нав. према: Жарковић, 2015: 171).

надзора подразумева забрану континуираног надгледања активности запослених. Ово не само због тога што континуирани надзор угрожава приватност запослених, већ и зато што представља озбиљан ризик за њихово психичко здравље и достојанство, због непријатног сазнања да су под сталном „присмотром“. 4) *Начело нужности* подразумева претходну процену могућности остваривања конкретних циљева применом мање инвазивних метода, односно утврђивање да те методе надзора нису могуће, односно довољне.

5. Закључак

На основу напред наведеног, могуће је закључити да широка употреба информационих технологија на раду отвара читав низ правних питања, а пре свега питање заштите права запослених на поштовање приватног живота. Теоријска, упоредноправна и судска решења указују да та питања, у највећем броју случајева, могу бити решена на основу постојећих правила која гарантују заштиту достојанства, поштовање приватног живота и заштиту података. Међутим, заштити запослених од прекомерне употребе разних техника и технологија на месту рада може допринети прецизније и строже уређивање актима аутономнога права. Својим интерним актима послодавац може потпуно забранити употребу службених средстава за комуникацију у приватне сврхе или је може ограничити. Без обзира за коју се опцију одлучи, послодавац мора поставити јасан и прецизан оквир приватности запослених на раду, јер паушално одређена ограничења по принципу „немогуће је да нисте знали“ не могу уживати заштиту. Право на поштовање приватног живота је елементарно људско право које се на раду може ускратити само у изузетним случајевима у којима је увођење мера надзора неопходно за заштиту законитих интереса послодавца, пре свега његове потребе да осигура безбедност и здравље на раду, заштити своју имовину и обезбеди правилно извршење престације рада. Одговарајућа контролна овлашћења послодавца, притом, морају бити ограниченог обима, тако да послодавац не би смео да надзире запослене на сваком месту и у сваком тренутку.

Литература/References

Бобан, М. (2012). Право на приватност и право на приступ информацијама у савременом информацијском друштву. Зборник радова Правног факултета у Сплиту. 3(2012). 575–598.

Georghe, M. (2017). Considerations of the conditions which the employer may monitor their employees at the workplace. *Juridical Tribune*. 2(2017). 62–69.

Даниловић, Ј. (2017). Право на приватност запослених. *Анали Правног факултета у Београду*. 2(2017). 162–182.

Димитријевић, П. (2011). Правна регулатива електронске комуникације и право на приватност. *Зборник радова Правног факултета Универзитета у Источном Сарајеву*. 2011. 199–2011.

De Hert, P. Loncke, M. Camera surveillance and workplace privacy in Belgium. Преузето 20. 6. 2018 <http://www.vub.ac.be/LSTS/pub/Dehert/017.pdf>

Ђукић, Д. (2017). Заштита података о личности са освртом на ново законодавство Европске уније у овој области. *Правни записи*. *Правни факултет Универзитета Унион*. 1(2017). 49–60.

Жарковић, И. (2015). Мере електронског надзора запослених и право на приватност на радном месту. *Наука, безбедност, полиција*. 3(2015). 165–182.

Јашаревић, С. (2016). Нове тенденције у области заштите личних података на раду у међународном праву. *Радно и социјално право*. 1(2016). 71–92.

Jourard, S. M. (1966). Some psychological aspects of privacy. *Law and Contemporary Problems*. 31(1996). 307–318.

Ковачевић, Љ. (2010). Радни однос и право на поштовање приватног живота. У Шундерић, Б, Лубарда, Б. и Јовановић, П. (Прир). *Остваривање и заштита социјалних права*, зборник радова са Саветовања правника. Београд. 166–184.

Ковачевић, Љ. (2013). Правна субординација у радном односу и њене границе. Београд.

Lugaresi, N. (2010). Electronic privacy in the workplace: Transparency and responsibility. *International Review of Law, Computers & Tecnology*. 163–173.

Miller, S. Weckert, J. (2000). Privacy, the workplace and the internet. *Journal of Business Ethics*. 28 (2000). 255–265.

Miller, C. Wells, S. Balancing Security and Privacy in the Digital Workplace. *Journal of Change Management*. 3–4(2007). 315–328.

Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology*, 17(1997). 147–156.

Прица, М. (2012). Ограничавање приватности државном интервенцијом заснованој на примени информационих технологија. Зборник радова Правног факултета у Нишу. LXII.2012. 445–462.

Roagna, I. (2012). Zaštita prava na poštovanje privatnog i porodičnog života, u skladu sa Evropskom konvencijom o ljudskim pravima. Vijeće Evrope. Strasbourg.

Snyder L, J. (2010). E-mail Privacy in the Workplace – A Boundary Regulation Perspective. *Journal of Business Communication*. 3(2010). 266–294.

Tolchinsky, P. D., McCuddy, M. K., Adams, J., Ganster, D. C., Woodman, R. W., & Fromkin, H. L. (1981). Employee perceptions of invasion of privacy: A field simulation experiment. *Journal of Applied Psychology*. 66 (1981). 308–313.

Tratar, B. (2017). Pravna osoba (persona ficta) kao titular ljudskog prava na privatnost – u Sloveniji i komparativno. *Pravni vjesnik: časopis za pravne i društvene znanosti Pravnog fakulteta Sveučilišta J.J. Strpssmayera u Osijeku*. 2(2017). 9–26.

Friedman A, B. Reed J, L. (2007). Workplace Privacy: Employee Realties and Legal Relations and Legal Implications of Monitoring Employee E-mail Use. *Empoy Respons Rights*. J(2007). 75–83.

Fusilier, M. R. Hoyer, W. (1980). Variables affecting perceptions of invasion of privacy in a personnel selection situation. *Journal of Applied Psychology*. 65(1980). 623–626.

Hendrickx, F. (2004). Employment privacy. U Blanpain, R. (Prir.). *Comparative labour law and industrial relations in industrialized market economies*. Kluwer Law International.

Halcrow, A. (2002). Navigating the New Landscape of Workplace Privacy Rights. *Employment Relations*. 1(2002). 45–53.

Hendrickx, F. (2002). Protection of Workers' Personal Data in the European Union. Leuven. Преузето 15.07.2018 file:///C:/Users/Milan/Downloads/1_data-protection-hendickx-combinedstudies_en%20(1).pdf

Warren D, S. Brandeis D, Louis. (1890). The Right to Privacy. *Harvard Law Review* IV. 5(1890). 193–220.

Westin F, A. (1967). Privacy and freedom. New York, NY: Atheneum. *Washington and Lee Law Review*. 1(1967). 166–170.

Westin F, A. (2003) Social and Political Dimensions of Privacy. *Journal of Social Issues*. 59(2)/2003. 431–453.

Пресуда Европског суда за људска права у случају *Niemietz v. Germany* од 16. децембра 1992 (представка 13710/88).

Пресуда Европског суда за људска права у случају *Halford v. the United Kingdom* од 25. јуна 1997. године (представка 20605/92).

Пресуда Европског суда за људска права у случају *Köpke v. Germany* од 5. октобра 2010. године (представка 420/07).

Пресуда Европског суда за људска права у случају *Bărbulescu v. România* од 5. септембра 2017. године (представка 61496/08).

Закон о раду (Сл. гласник РС, бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 – одлука УС и 113/2017).

Закон о заштити података (Сл. гласник РС, бр. 97/2008, 104/2009 – др. закон 68/2012 – одлука УС и 107/2012).

Marija Dragičević, LL.M.

Teaching Assistant,

Faculty of Law, University of Niš

MODERN TECHNOLOGIES AND EMPLOYEES' RIGHT TO RESPECT FOR PRIVATE LIFE

Summary

Modern technologies are a consequence of the significant development of human thought and inventiveness. Individuals, legal entities and countries depend on using modern technologies which enable them to perform different tasks, do business or offer a large number of services. In recent years, the use of information technology has spread rapidly in different areas, including the workplace. Apart from the undisputable contribution to the effective exercise of the employer's authorities, the development of information technologies has opened up a number of issues concerning the possibility of providing the necessary presumptions to ensure the adequate protection of the legitimate interests and rights of parties involved in labour relations. Both the employer and the employees may be exposed to potential danger of unauthorized disclosure and abuse of confidential data or private information. Thus, on the employer's part, there is a concern that certain data (e.g. relating to confidential activities of a company, financial transactions, personnel management, and employees' personal data) may be misused by unauthorized entities, which creates the need for installing devices for data protection and monitoring access to such data. In addition, employers justifiably fear that employees may use modern technology for private purposes during working hours. On the other hand, employees are mainly concerned about the danger of misusing modern technologies for the purpose of monitoring and supervising the performance, as well as certain aspects of private life, which opens the issue of the employees' right to privacy and right to respect for private life.

In this context, the author discusses the question of permissible use of modern technologies, particularly in light of the protection of human rights and fundamental freedoms of employees. As the central problem, the author analyzes the issue of the difficulty of striking a balance between the employer's interest to ensure the workplace safety and the healthy working conditions and, on the other hand, the employees' interest to ensure respect for their privacy rights and dignity at work. In particular, the author focuses on specific control measures aimed at monitoring the use of official means of communication and video surveillance.

Keywords: *right to privacy, employees, right to respect for private life, modern technologies.*

