Др Жељко Мирјанић,*
Редовни професор Правног факултета,
Универзитет у Бањој Луци, Република Српска
Босна и Херцеговина

ОРИГИНАЛНИ НАУЧНИ РАД
10.5937/zrpfn0-23398

UDK: 349.2:342.7]:004.738.5
342.7
Рад примљен: 30.09.2019.
Рад прихваћен: 05.12.2019.

ЗАШТИТА ЛИЧНИХ ПОДАТАКА ЗАПОСЛЕНИХ У УСЛОВИМА КОРИШТЕЊА ИНФОРМАЦИОНИХ ТЕХНОЛОГИЈА

Апстракт*: Послодавац путем информационих технологија прикупља, обрађује, користи и чува личне податке запослених потребне за остваривање права и обавеза у радном односу, а запослени има право на заштиту података у току и послије престанка радног односа. Да би се обезбиједила заштита личних података и приватности запослених, неопходно је дати већи значај правном уређивању начина коришћења ових технологија. Поред увећања ризика од злоупотребе личних података усљед употребе ових технологија, и потребе да се промијени правна пракса да запослени ријетко користе право на заштиту личних података, као важан разлог за правно уређивање може се издвојити обавеза постепеног усклађивања домаћег права са правом Европске уније (према Споразуму о стабилизацији и придруживању). Наведени разлози утичу да преовладава став да је неопходно уградити европске стандарде из ове области, предвиђене Уредбом (ЕУ) 2016/679 Европског парламента и Савјета из 2016. о заштити појединаца у вези с обрадом личних података и о слободном кретању таквих података. Тема текста обухвата и утицај информационих технологија на заштиту личних података запослених „узбуњивача".*

Кључне ријечи*: заштита приватности и личних података запослених, утицај информационих технологија на заштиту личних података, заштита запослених узбуњивача.*

* zeljko.mirjanic@pf.unibl.org

1. Увод

Заштита личних података запослених у условима кориштења информационих технологија представља посебну тему у оквиру радног права и дио шире правне теме о заштити основних права и слобода грађана у прикупљању, обради, кориштењу и чувању личних података. У оквиру правних истраживања, заштита личних података (података о личности) може се истраживати са аспекта појединe или више правних научних дисциплина унутар једне или више ужих правних научних области, као питање унутрашњег, европског и међународног права. Заштита личних података у условима кориштења информационих технологија представља поред теме правних истраживања, тему информатичких и других истраживања у разним научним областима и научним пољима и тему интердисциплинарних истраживања. У доступној правној литератури недостају резултати пројектних истраживања о заштити личних података и о повезаности права и информатике. Изабрана тема указује на значај истраживања ове везе засноване на томе да су информационе технологије незамјењиво средство за обраду података. Пред истраживачима је задатак да објасне промјене у области заштите личних података и заштите приватности усљед кориштења информационих технологија које олакшавају обраду, а отежавају чување података и заштиту приватности. Изгледа оправдана констатација да је потреба за сигурношћу информација на мрежи једнака потреби за печатирањем воском стратешки важних докумената у претходној ери комуникација „на папиру" (Васковић, 2014: 40). Заштита личних података запослених у условима кориштења информационих технологија је једна од тема које се могу поставити по питању утицаја информационих технологија на промјене у свијету рада и на радне односе. Као друге актуелне и неистражене теме могу се издвојити рад на даљину, заштита безбједности и здравља запослених који користе ове технологије, итд.

Правно регулисање заштите личних података и приватности запослених се заснива на уставној заштити података о личности којом је забрањена и кажњива употреба тих података изван сврхе за коју су прикупљени, праву свакога да буде обавијештен о прикупљеним подацима о својој личности и праву на заштиту од њихове злоупотребе. Тренд да послодавци све више и масовно користе информационе технологије, подстакнут ефикасношћу и финансијском доступношћу ових технологија, упућује на питање како законским и аутономним правним одредбама правно регулисати кориштење ових технологија у циљу остваривања уставних одредби. Потребно је избјећи повреду безбједности личних података запослених која доводи до уништења, губитка, измјене, неовлашћеног

откривања или приступа подацима. Да би се то избјегло, послодавац је дужан да регулише, организује и контролише обраду података запослених на начин који спречава кршење њихових права и злоупотребе. Полазећи од става да треба регулисати кориштење информационих технологија код послодавца на начин да се обезбиједи заштита података о личности и приватности запослених према конкретним условима рада, може се поставити и теза да је заштита личних података и приватности запослених важна тема за колективне преговоре и социјални дијалог. При томе се полази од схватања да се заштита личних података и приватности не може посматрати одвојено од заштите достојанства на раду и да је људско достојанство данас стандардни садржај европских устава, било самостално или као додатак уз људска права (право на живот, приватност, морални интегритет, идентитет или правичност кривичног поступка) (Čulo, 2015: 50). Договором социјалних партнера могу се постићи ефикасно и рационално кориштење ових технологија и избјећи радни спорови, а посебно спорови поводом видео-надзора и надзора електронске поште, те утицати на свијест запослених и послодаваца. Поред законом утврђених легитимних разлога за увођење видео-надзора у просторијама послодавца, ове разлоге би заједнички могли утврдити и социјални партнери онда када то налаже оправдан интерес послодавца. Но, моћ колективног дјеловања радника није значајније кориштена за заштиту њихових основних људских права на раду, укључујући и право на приватност. Имајући у виду да је савремена технологија омогућила послодавцу да на веома брз и лак начин прикупља и обрађује податке о запосленом и да их континуирано надзире, било би добро да представници радника редефинишу своју улогу у погледу заштите права радника (Ковач Орландић, 2019: 174).

На заштиту личних података запослених примјењују се поједине одредбе из радног законодавства и одредбе закона који регулише заштиту личних података (података о личности), те се поставља питање усклађености заштите података запослених са начелима и правилима заштите личних података која се односе на све грађане, а која су обично написана по узору на европске и међународне стандарде у овој области. Поред ових стандарда, за регулисање заштите личних података и заштите приватности запослених важни су ставови Европског суда за људска права садржани у пресудама које се односе на заштиту личних података и приватности**.** У овом тексту се полази од опште тезе да је за унапређење нивоа заштите личних података и приватности запослених важно уградити у законске одредбе међународне и европске стандарде из ове области, а разлози за то су повезани са успостављањем информатичког друштва у околностима глобализације и регионализације. У прилог томе може се навести да је у Преамбули

Декларације МОР-а о социјалној правди у циљу праведне глобализације констатовано да садашњу глобализацију карактерише распрострањеност нових технологија и да је она фактор који изазива преобликовање свијета рада из корјена, те да МОР у контексту глобализације мора, између осталог, да промовише филозофију постављања стандарда, као основног елемента својих активности, повећањем њиховог значаја на свијет рада.[1] Под утицајем актуелне фазе глобализације, започете у прошлом вијеку, мијења се и начин заштите људских права, укључујући права запослених и у оквиру тога право на заштиту личних података и приватности. У литератури се обично под утицајем глобализације на стандарде у међународном и европском праву подразумијева неолиберална промјена свијета током претходних деценија. У научној јавности нису до краја разјашњене дилеме о природи, значају и посљедицама актуелне фазе процеса глобализације и европске интеграције као дијела тог процеса и утицај који ови процеси имају на промјене правног система у (пост)транзиционим земљама Југоисточне Европе. У јавности није спорно да се идеја неолибералне глобализације разликују од идеје глобализације као историјског процеса, чији је саставни дио развој међународног права у правцу остваривања прокламованих универзалних вриједности, укључујући развој међународног радног права у правцу остваривања циљева радног права као што су социјална правда, социјални мир и забрана конкуренције. Даљи ток глобализације и карактер њеног утицаја на развој (радног) права није могуће сигурно предвидјети, иако је почетком овог вијека изгледало друкчије. За земље Југоисточне Европе усклађивање домаћег права са правом ЕУ представља континуиран и дуготрајан процес у оквиру европске интеграције. Динамика и обим усклађивања објективно зависе од могућности поједине земље да се приближи степену економског и социјалног развоја ЕУ, а субјективно зависи од капацитета институција власти и воље друштвених партнера да према достигнутом степену развоја земље креирају промјене одређених грана права (Мирјанић, 2014: 130). Али, дуготрајност процеса европске интеграције доноси овим земљама неизвјесност и успорава динамику усклађивања права.

У тексту се полази и од тезе да обим заштите личних података предвиђен за запослене није довољан да се заштите запослени узбуњивачи и да је важна додатна заштита идентитета ових лица стога што ове технологија омогућавају лакше откривање личних података узбуњивача.

1 Декларација МОР-а о социјалној правди у циљу праведне глобализације, енг. *Declaration on Social Justice for a Fair Globalization, ILC, 97th session,Geneva, 2008.*

2. Европски стандарди заштите личних података

Регулисање коришћења информационих технологија за обраду личних података, укључујући и обраду личних података запослених, у земљи кандидату за пријем у Европску унију јесте важан дио процеса усклађивања (хармонизације) права. Као примјери те обавезе могу се навести члан 81 Споразума о стабилизацији и придруживању који је закључила Република Србија са Европском унијом, који успоставља обавезу да се усклади законодавство које се односи на заштиту података о личности са законодавством Уније,[2] и члан 79 Споразума о стабилизацији и придруживању који је закључила Босна и Херцеговина, а који исто успоставља обавезу усклађивања законодавства које регулише заштиту личних података са правом Заједнице и другим европским и међународним стандардима, те обавезу да се успостави независно надзорно тијело са довољним финансијским и људским потенцијалима у циљу ефикасног праћења и гарантовања провођења законодавства о заштити личних података.[3] Земље у региону у законском регулисању заштите личних података уважавају европске стандарде за заштиту података и постепено са различитом динамиком испуњавају преузету обавезу хармонизације. Тако је Република Србија донијела Закон о заштити података о личности послије доношења Уредбе Европске уније 2016/679, за разлику од Босне и Херцеговине која још није ускладила закон који регулише заштиту личних података са овом Уредбом, а што није посљедица друкчијег односа према преузетој обавези, већ динамике законодавне дјелатности.[4] Основне одредбе о усклађивању националних прописа с правном стечевином ЕУ садржане су у Уговору о оснивању Европске заједнице, а што се односи и на процес усвајања и примјене права ЕУ у радном праву и свијету рада. Како је подвучено, правна стечевина није само право у ужем смислу, јер обухвата садржај, начела и политичке циљеве оснивачких уговора, законодавство усвојено на темељу оснивачких уговора, пресуде Европског суда правде, декларације и резолуције ЕУ, мјере које се односе на заједничку спољну и безбједносну политику, правосуђе и унутрашње послове, међународне уговоре које је склопила Европска заједница, као и уговоре закључене између држава чланица с трећим земљама у подручју дјеловања ЕУ

2 Закон о потврђивању Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије, са друге стране, Сл. гласник РС-Међународни уговори, 83/08.

3 Одлука о ратификацији Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица и Босне и Херцеговине, *Сл. гласник БиХ – Међународни уговори*, 10/08.

4 Закон о заштити података о личности, Сл. гласник РС, 87/18; У Црној Гори: Закон о заштити података о личности, Сл. лист ЦГ,79/08, 70/09, 44/12 и 22/17.

(Učur, 2007: 311). Обавеза усклађивања права утврђена појединачним Споразумима о стабилизацији и придруживању између Европске заједнице и земаља Југоисточне Европе испуњава се постепеним промјенама права које треба да помири европске захтјеве са домаћим правним, економским и социјалним околностима.

Законодавац у регулисању заштите података о личности и приватности полази од стандарда у које је уграђен концепт приватности успостављен током развоја европског правног оквира за заштиту података, а који почиње са Европском конвенцијом за заштиту људских права и основних слобода (чл. 8), преко Повеље Европске уније о основним правима која регулише заштиту независно од облика у коме су садржани и медијума на коме су похрањени подаци, других извори права ЕУ који уређују заштиту података, Директиве 95/46/ЕЗ и завршава Уредбом 2016/679 о заштити појединаца у вези с обрадом личних података и о слободном кретању таквих података. Заштита личних података предвиђена је најважнијим актима Европске уније као основно право: према Уговору о функционисању Европске уније (члан 16) свако има право на заштиту својих личних података, а према Повељи Европске уније о основним правима (члан 8) свако има право на заштиту личних података; подаци морају се обрађивати поштено, у утврђене сврхе и на основу сагласности лица о коме је ријеч, или на некој другој легитимној основи утврђеној законом; свако има право на приступ прикупљеним подацима који се на њега или њу односе и право на њихово исправљање; поштовање тих правила подлијеже надзору независног тијела. Како примјећују аутори, у општој еволуцији концепта приватности, постепено је успостављено право на приватност, тако што је препознавање и признавање права на приватност настало из потребе да се обезбиједе што ефикаснији механизми приватности јер су, са друштвеним и технолошким напретком, могућности њене повреде постале све доступније, а начини на који се те повреде чине све софистицираније (Поповић, Јовановић, 2017: 123).

За регулисање заштите личних података у процесу усклађивања домаћег права са правом Европске уније посебна важност припада Уредби 2016/679 Европског парламента и Савјета од 27. априла 2016. о заштити појединаца у вези с обрадом личних података и о слободном кретању таквих података, те о стављању изван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података)[5], чија је примјена обавезна за чланице од 25. маја 2018. године.

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal L 119(1).

Она ставља ван снаге Директиву 95/46/ЕЗ донијету 1995. године када је интернет још био у повојима и, с обзиром на дигитално доба у којем се биљежи рапидан развој технолошких достигнућа која омогућавају пуно бржи проток роба и услуга, и размјену података, циљ доношење Уредбе је било осигурање једнаковриједног нивоа заштите појединаца и слободног протока личних података широм Европске уније (Bet-Radetić, 2017: 9). Према Уредби, начела и правила о заштити појединаца у вези с обрадом личних података поштују основна права и слободе. Општа уредба о заштити података се примјењује директно без могућности интерпретација, а што свим европским грађанима обезбјеђује уједначено право на заштиту личних података. Као један од разлога за уређивање заштите личних података у Европској унији наводи се нужност доношења правног инструмента који ће осигурати заштиту права и личних слобода појединаца у вези с обрадом личних података.[6] Она се примјењује на фирме и појединце који обављају одређену професионалну активност, удружења, болнице, клубове, на физичка лица када обрађују личне податке изван оквира потреба домаћинства, на државне институције (осим у случајевима кривичноправних активности, попут спречавања кривичних дјела или прогона починилаца истих, те у подручјима изван надлежности права Европске уније). Општа уредба о заштити података се сматра веома значајним кораком у правцу успостављања јединственог дигиталног тржишта у Европској унији, и ствара савременији и детаљнији оквир за правно уређење заштите података о личности (Поповић, Јовановић, 2017: 137). Правила која она садржи служе као примјер у земљама ван Уније, као што је, на примјер, правило да грађани имају надзор над обрадом властитих података. Општа уредба о заштити података као и Директива 95/46/ЕЗ садржи право на обавијештеност, право на приступ подацима, право на протест лица чији се подаци обрађују, а садржи и нова права: право да се ограничи обрада и право на преносивост података.

Општа уредба о заштити података оставља могућност земљама чланицама да у случајевима обраде података запослених пропишу посебна правила за обраду личних података у оквиру запослења. То се првенствено односи на услове под којима се лични подаци могу обрађивати на основу сагласности запосленог за потребе запошљавања, извршавања уговора

6 У прилог томе, може се навести да у извјештају из 2010. године Агенције ЕУ за основна права, у коме се говори о потреби заштите личних података запосленог лица као субјекта у неравноправном положају, наводи да су у земљама чланицама уочене различите неправилности у погледу заштите личних података. European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities*, преузето 28. 9. 2019. http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf , стр. 37.

о раду, испуњавања законом или колективним уговорима утврђених обавеза. У питању су управљање, планирање и организација рада, заштита здравља и безбједности на раду, остваривање права из радног односа и престанак радног односа. Према овој Уредби, да би био могућ надзор, потребно је да послодавац то уреди општим актом чији су предмет услови, кориштење и надзор службене електронске поште, службених мобилних телефона, кориштење биометријских података и сл. Видео-надзор није директно неведен у Уредби, али кроз дефиницију личних података посебно осјетљиве природе даје му се значај надзора за који су потребне посебне мјере заштите, односно она снимак са видео-надзора класификује као лични податак посебно осјетљиве природе. Кориштењем видео-надзора могу се обрађивати лични подаци посебно осјетљиве природе, као што су подаци о етничком поријеклу, здравственом стању, економски и социјални статус, итд. Постављање видео-надзора је право власника некретнине, али видео-надзор намијењен да се обезбиједи сигурност лица и имовине не може да се постави на начин да се крши право запосленог на приватност. Околности могу оправдати видео-надзор ако вриједност добара која се желе заштитити и степен угрожености који пријети преовладава у односу на заштиту личних података. Поред наведеног, за регулисање начина кориштења видео-надзора, прихватљивости надзора електронске поште и сл. важне су пресуде Европског суда за људска права донесене поводом повреде заштите личних података и приватности запослених. Пресуде овог Суда утичу на формирање правних схватања о правима и одговорности послодавца и запосленог у вези са заштитом личних података. Пракса Суда показује да кориштење информационих технологија прати кршење права на заштиту права приватности, конкретно члана 8 о заштити података и приватности Европске конвенције за заштиту људских права и основних слобода, а по коме свако има право на поштовање свог приватног и породичног живота, дома и преписке, и држава се неће мијешати у вршење овог права осим ако то није у складу са законом и ако је то неопходно у демократском друштву у интересу националне и јавне безбједности, економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, заштите права и слобода других. Као примјер могу се издвојити пресуде у предмету Копланд (Copland) против Уједињеног Краљевства[7] и предмету Лопез Рибалда (López Ribalda) и други против Шпаније[8]. Први судски предмет се односи на услове под којима послодавац може да надзире кориштење телефона, електронске поште и интернета на послу и важност да се регулише праћење и истакне

7 *Copland v. United Kingdom*, Judgment of 3 April 2007, no. 62617/00.

8 *López Ribalda and others v. Spain*, Judgment of 9 January 2018, no. 8567/13.

упозорење запосленима о праћењу, а други судски предмет се односи на тајно праћење уз помоћ видео-надзора. Према пресуди донесеној 2007. године у предмету Копланд (Copland) против Уједињеног Краљевства, прикупљање и чување личних података о телефонским позивима, коришћењу електронске поште и интернета без знања подносиоца јесте повреда права на поштовање приватног живота и преписке. Суд је закључио да су телефонски позиви упућени са посла покривени појмом „приватни живот" и „преписка" у смислу члана 8 Конвенције, као и да се то односи на коришћење електронске поште и интернета, а при чему је небитна чињеница да подаци нису објављени или употребљени против подносиоца пријаве у дисциплинском или другом поступку. У периоду на који се представка односи ни у домаћем законодавству ни у актима послодавца није било прописа о томе под којима условима послодавац може да надгледа како запослени користе телефон, e-mail и интернет, те да се не може третирати да је мијешање у приватни живот било „у складу са законом" као што захтијева члан 8, став 2 Конвенције. Суд не искључује могућност да се праћење коришћења телефона, електронске поште или употребе интернета на радном мјесту може сматрати „неопходним у демократском друштву" у одређеним ситуацијама када постоји легитиман циљ. У предмету Лопез Рибалда (López Ribalda) и други против Шпаније је повријеђено право на приватност зато што подносиоци, упркос законским одредбама, нису упозорени да су током читавог радног времена под видео-надзором, иако су ухваћени скривеним камерама да краду због чега су добили отказ. Европски суд је закључио како, без обзира на то што је за спорни видео-надзор одговоран власник приватне фирме, држава има позитивну обавезу успоставити одговарајућу равнотежу између заштите приватног живота грађана и интереса послодавца. Према шпанском закону, појединце се мора на јасан начин обавијестити о прикупљању и обради личних података. Европски суд је утврдио да је видео-надзором повријеђено право на приватни живот подносилаца, али је оцијенио да коришћењем снимака надзорне камере у судском поступку није повријеђено право на поштено суђење у радном спору, јер су, међу осталим, осим снимака кориштени и други докази.

3. Регулисање заштите личних података запослених

Заштита личних података и приватности запослених је регулисана у оквиру заштите права запослених, а може се теоријски посматрати и као дио заштите здравља и безбједности на раду у ширем смислу. Како се наводи, заштита здравља и безбједности на раду у ширем смислу, поред скупа мјера и средстава којима су циљ безбједни услови рада (заштита у

ужем смислу), обухвата и скуп мјера и средстава за стварање удобности на мјестима рада, хумане радне средине, очувања приватности, људског достојанства и моралног интегритета запосленог на раду. Појам заштита здравља и безбједности на раду у ширем смислу треба да створи свим категоријама запослених физичко и ментално здравље, заштити морални интегритет и достојанство личности, пружи задовољство и удобност на послу. Мјере заштите приватности запосленог треба сагледати и у контексту (не)допуштености вођења евиденција о личности запосленог које нису у вези са пословима радног мјеста (Лубарда, 2013: 145). Колико је важно регулисати мјере заштите приватности показује примјер заштите података о физичком или менталном здрављу, укључујући и податке о пружању здравствених услуга, који откривају информације о здравственом стању. Како је констатовано, послодавац има легитимно право да буде обавијештен о здравственом стању запосленог на радним мјестима са повећаним ризицима на основу периодичних љекарских прегледа, како би могао предузети мјере заштите здравља и безбједности на раду (Лубарда, 2013: 146). Послодавац може да упути запосленог на одговарајуће прегледе у здравствену установу ако одбије оцјену здравствене способности, а ради на пословима за чије је обављање као посебан услов утврђена посебна здравствена способност, али може да то учини и у случају ако запослени не достави потврду о привременој спријечености за рад или злоупотријеби право на одсуство за вријеме привремене спријечености за рад.[9] У овом случају упућивање запосленог на одговарајуће прегледе у здравствену установу служи да се утврди да ли постоји разлог за отказ уговора о раду. Коришћење информационих технологија отежава чување података о здравственом стању и других „осјетљивих" личних података и увећава опасност од тога да подаци буду неправилно кориштени или злоупотријебљени. Стога је важно обезбиједити цјеловитост и повјерљивост да се подаци обрађују на начин којим се постиже одговарајући ниво безбједности, укључујући заштиту од неовлашћене или незаконите обраде, те од случајног губитка, уништења или оштећења, а што тражи и Уредба (ЕУ) 2016/679.

Предмет одредби у радном законодавству је прикупљање, коришћење, чување и заштита личних података потребних за закључивање уговора о раду, за остваривање права у радном односу, за заштиту безбједности и здравља на раду, итд. Послодавац може користити ове податке послије престанка радног односа зависно од дужине времена у коме је неопходно да се они користе због одређеног разлога, као што је стицање права на пензију, регулисање здравственог осигурања, итд. У прилог наведеног

9 Члан 179 Закона о раду Републике Српске, *Сл. гласник РС*, 1/16.

ограничења може се навести правило у препоруци Савјета Европе да не треба чувати личне податке дуже него што оправдава сврха обраде или захтијевају интереси садашњег или бившег запосленог лица,[10] као и то да према Уредби Европске уније 2016/679 подаци морају бити чувани тако да је могућа идентификација испитаника само толико времена колико је потребно у сврху ради које се лични подаци обрађују, а даља обрада података је могућа ради архивирања у јавном интересу, истраживања и статистичке обраде. Анализирани закони о раду прописују које податке послодавац не може тражити, а које податке обрађује уз право запосленог да оствари увид, захтијева исправљање нетачних и брисање података који нису од непосредног значаја за послове које обавља.[11] То је у складу са Уредбом (ЕУ) 2016/679, према којој подаци морају бити тачни и ажурни и морају се предузети мјере да се лични подаци који нису тачни, узимајући у обзир сврху за коју се обрађују, без одлагања избришу или исправе. Запослени може ускратити одговоре на питања која крше приватност и достојанство (питања која се односе на брачни статус, сексуалну оријентацију, мајчинство и планирања породице, итд.). Послодавцу није допуштено да захтијева непотребне податке који откривају приватни живот запосленог, али и поред те забране и права запосленог да тражи брисање сувишних и исправљање нетачних података, да тражи заштиту ако послодавац непрописно користи информационе технологије, запослени није у равноправном односу са послодавцем ни у погледу обраде личних података. Поред правних прописа, како се наводи, правни основ за обраду личних података радника од стране послодавца налази се у склапању и извршењу уговора о раду. Уговори о раду се заснивају на добровољној основи између радника и послодавца, па можемо казати да се радни однос заснива и на међусобном повјерењу између послодавца и радника, али никако не смијемо занемарити да је послодавац у односу на радника у супериорнијим положају (Bet-Radetić, 2017: 4). У прилог томе, може се навести да посљедица коришћења електронског надзора може бити дисциплинска мјера или отказ од стране послодавца ако се путем надзора докаже да је запослени учинио тежу повреду радне обавезе, да није поштовао радну дисциплину, да постоји оправдан разлог за отказ уговора о раду. У овом случају коришћење информационих технологија служи да се утврди да ли запослени испуњава дужности због чијег кршења

10 Council of Europe, *Rec No. R (89) 2 of the Committee of Ministers to Member States on the Protection of Personal Data used for Employment Purposes*, 18. 01. 1989. godine.

11 Закон о раду, *Сл.гласник Републике Србије*, 24/05, 61/05, 54/09, 32/13, 75/14, 13/17,113/17 и 95/18. Закон о раду, Сл. гласник Републике Српске, 1/16 и 66/18; Закон о раду, *Сл. новине ФБиХ*, 26/16 и 89/18; Закон о раду, *Сл. лист ЦГ*, 49/08, 26/09, 88/09, 26/10, 59/11, 66/12, 31/14, 53/14 и 4/18; Zakon o radu, *Narodne novine,* 93/14 и 127/17.

може да престане радни однос, као што су забрана дискриминације, дужност да обавијести послодавца о битним околностима које утичу на обављање послова, односно о потенцијалној опасности за живот и здравље, на опасности од настанка материјалне штете, итд. Да би се заштитила приватност запослених, послодавац је дужан да регулише коришћење електронског надзора запослених и да обавијести запослене и њихове представнике о томе, начину обраде и заштите података. Уз нужност свеобухватног нормативног регулисања електронског надзора законским текстом, поједина питања би се могла додатно уредити и интерним актима послодаваца. Надзор треба користити само у случају остваривања легитимних циљева, он мора бити транспарентан, сразмеран и нужан. Интерни акти послодавца треба да садрже одредбе којима се јасно дефинишу поље примјене, циљеви и разлози увођења система надзора, а са увођењем мјера електронског надзора морали би се сложити и запослени (Жарковић, 2015: 179).

Право на заштиту личних података и приватности запослених не може се посматрати одвојено од права на заштиту података о личности (личних података грађана), које означава заштиту приватности лица у ширем смислу, односно свега онога што неко лице одређује и по чему се оно разликује од других лица. Поред закона који чине радно законодавство, на заштиту личних података запослених се примјењују одредбе закона који регулише заштиту личних података, уз обавезу да посебни закони буду у складу са општим. За регулисање заштите личних података запослених вриједе начела обраде података утврђена општим законом о заштити личних података: подаци се морају обрађивати законито, поштено и транспарентно у односу на лице на које се подаци односе, подаци морају бити тачни и, ако је то неопходно, ажурирани, прикупљање података је ограничено у односу на сврху обраде, врши се минимизација података, ограничење чувања, поштују интегритет и повјерљивост.[12] Према Закону о заштити података о личности у Републици Србији (чл. 91), на обраду у области рада и запошљавања примјењују се одредбе закона којима се уређује рад и запошљавање и колективни уговори, уз примјену одредби овог закона. Ако закон који уређује рад и запошљавање или колективни уговор садрже одредбе о заштити података о личности, морају се прописати и посебне мјере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размјену података о личности унутар мултинационалне компаније, односно групе привредних субјеката,

12 Члан 5 Закона о заштити података о личности, *Сл. гласник РС, 87/18.*

као и систем надзора у радној средини.[13] На који начин коришћење информационих технологија увећава опасност од штетних посљедица за запослене указује и профилисање облика аутоматизоване обраде, које се користи да би се оцијенило одређено својство личности, посебно у циљу анализе или предвиђања радног учинка физичког лица, његовог економског положаја, здравственог стања, личних склоности, интереса, поузданости, понашања, локације или кретања. [14] Лице на које се подаци односе има право да се на њега не примјењује одлука донијета искључиво на основу аутоматизоване обраде, укључујући и профилисање, ако се том одлуком производе правне посљедице по то лице или та одлука значајно утиче на његов положај, осим у законом одређеним случајевима.[15]

У земљама у региону је прихваћен нормативни приступ да је неопходно посебно уредити заштиту лица која пријаве корупцију како би учествовали у заштити јавних интереса, што показују доношење закона чији је циљ и предмет заштита узбуњивача.[16] У питању је заштита радноправне сигурности лица која воде борбу против корупције ризикујући да буду шиканирани од стране послодавца. Законско регулисање заштите права узбуњивача, по узору на законе у појединим европским државама, може из нове законодавне праксе прерасти у нормативни тренд у региону. Заштита радноправног статуса запослених који открију информације о корупцији и другим незаконитим радње код послодавца је обезбијеђена у оквиру заштите права која припада свим запосленим и без законског регулисања заштите узбуњивача, али постепено преовладава став да та заштита није довољна. Ризик од корупције је појачан у оним срединама гдје није пружена одговарајућа заштита узбуњивача (Мирјанић, Чошабић, 2016: 132). Заштита идентитета и личних података ових лица је додатно угрожена у условима коришћења информационих технологија, а као примјер за то може се навести псеудонимизација, а под којом се подразумијева обрада података на начин који онемогућава приписивање података о личности одређеном лицу без коришћења додатних података, а под условом да се додатни подаци чувају посебно и да су предузете техничке, организационе и кадровске мјере које обезбјеђују да се податак о личности не може приписати одређеном или одредивом лицу.[17]

13 Члан 91 Закона о заштити података о личности, *Сл. гласник РС, 87/18.*

14 Члан 4 Закона о заштити података о личности, *Сл. гласник РС, 87/18.*

15 Члан 38 Закона о заштити података о личности, *Сл. гласник РС, 87/18.*

16 Закон о заштити узбуњивача, *Сл. гласник РС, 128/14;* Закон о заштити лица која пријављују корупцију у институцијама Босне и Херцеговине, *Сл. гласник БиХ, 100/13;* Закон о спрјечавању корупције, *Сл. лист ЦГ*, 53/14 и 42/17.

17 Члан 4 Закона о заштити података о личности, *Сл. гласник РС, 87/18.*

Псеудонимизација може смањити ризик од повреде личних података. Када се информационе технологије користе за пријављивање корупције од стране запослених, чак и ако се не захтијевају очигледни лични подаци, тијело којем се врши пријава мора водити рачуна о томе да се и IP адреса сматра личним податком, јер је у пресуди Суда правде Европске уније у предмету Breyer против Њемачке одлучено да чак и динамична IP адреса може у одређеним околностима представљати лични податак (Mirjanić, Čošabić, 2017: 135).

4. Закључак

Послодавци користе информационе технологије за контролу присуства запослених на радном мјесту, за заштиту безбједности и здравља на раду, за заштиту имовине и смањења ризика од насиља и крађа, итд. Стога је важна тема како законски регулисати коришћење нових технологија на начин да се обезбједи заштита личних података и приватности, који су угрожени усљед ширења праксе електронског надзора, софистицираног праћења запослених који раде на рачунару и прикупљања биометријских података запослених. Посматрана тема обухвата и питање заштите личних података запослених узбуњивача. Регулисање коришћења информационих технологија за обраду личних података је и важан предмет колективног уговора, општег акта послодавца и других облика аутономног правног регулисања по питањима која нису регулисана законом. То се односи на аутономно регулисање услова за коришћења и начин њиховог коришћења за обраду личних података који се траже ради закључивања уговора о раду и током трајања радног односа, као и других питања која се односе на заштиту личних података. Задатак правника је да, стварањем правних прописа и успостављањем правне праксе, одреде границу између права запослених на заштиту личних података и приватности и права послодавца да обрађује личне податке и за то користи информационе технологије. Уз афирмацију права на приватност и правну заштиту тог права, неопходно је развијање свијести о значају поштовања приватности запослених. За унапређење нивоа заштите личних података и приватности запослених важно је уградити у законске одредбе међународне и европске стандарде из ове области. Поређење законских одредби о заштити података о личности у земљама региона показује да се уважавају европски стандарди за заштиту података и постепено испуњава обавеза хармонизације права. У том смислу, прилагођавање законодавства најважнијим промјенама које доносе информационе технологије, укључујући и промјене у свијету рада, зависи од развоја европског права и права Европске уније које има за циљ да одреди права појединаца и обавезе субјеката који обрађују личне податке.

Литература/References

Bet–Radetić B. (2017). Zaštita osobnih podataka u radnim odnosima, *Radno pravo***.** 9/17.

Васковић, В. (2014). *Електронско пословање у јавној управи eGoverment***,** Београд: Београдска пословна школа.

Жарковић, И. (2015). Мере електронског надзора запослених и право на приватност на радном месту. *Наука, безбедност, полиција***.** 20(3), 165–182.

Ковач Орландић, М. (2019). Видео-надзор у просторијама послодавца. *Зборник Правног факултета у Нишу***.** 82/19. 165–182.

Лубарда, Б. (2013). *Увод у радно право***.** Београд: Правни факултет Универзитета у Београду.

Мирјанић, Ж. (2014). Значај социјалног дијалога у процесу усклађивања домаћег права са правом Европске уније. *Зборник радова Правног факултета у Нишу***.** 68/14. 129–143.

Mirjanić, Ž. Čošabić, J. (2016). Protection of whistleblower's employment status, *International Scientific Conference on Economic and Social Development – The Legal Challenges of Modern World.* 130–139.

Mirjanić, Ž. Čošabić, J. (2017). Advantages and Disadvantages of the Information Technology Use in the Whistleblowing Process, *22nd International Scientific Conference on Economic and Social Development – "Legal Challenges of Modern World".* 130–138.

Поповић, Д. Јовановић, М. (2017). *Право интернета: одабране теме*. Београд: Правни факултет Универзитета у Београду.Učur, M. (2007) *Nomotehnika*, Rijeka: Veleučilište u Rijeci.

Čulo, I. (2015) Pravo na dostojanstvo u radu – međunarodni i evropski standardi. *Radno pravo* 3/15. 50–58.

European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities*, преузето 28. 9. 2019. http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf .

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal L 119(1).

Declaration on Social Justice for a Fair Globalization, ILC, 97th session,Geneva, 2008.

Закон о потврђивању Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије, са друге стране. *Сл. гласник РС – Међународни уговори*. Бр. 83/08

Одлука о ратификацији Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица и Босне и Херцеговине. *Сл. гласник БиХ – Међународни уговори*. Бр. 10/08

Закон о заштити података о личности. *Сл. гласник РС*. Бр. 87/18.

Закон о заштити података о личности. *Сл. лист ЦГ*. Бр. 79/08, 70/09, 44/12 и 22/17.

Закона о раду Републике Српске. *Сл. гласник РС*. Бр. 1/16 и 66/18.

Закон о раду. *Сл.гласник Републике Србије*. Бр. 24/05, 61/05, 54/09, 32/13, 75/14, 13/17,113/17 и 95/18.

Закон о раду. *Сл. лист ЦГ*. Бр. 49/08, 26/09, 88/09, 26/10, 59/11, 66/12, 31/14, 53/14 и 4/18.

Zakon o radu. *Narodne novine.* Бр. 93/14 и 127/17.

Закон о заштити личних података. *Службени гласник БиХ. Бр.* 49/06, 76/11 и 89/11.

Закон о заштити узбуњивача. *Сл. гласник РС*. Бр. 128/14.

Закон о заштити лица која пријављују корупцију у институцијама Босне и Херцеговине. *Сл. гласник БиХ. Бр. 100/13.*

Закон о спрјечавању корупције. *Сл. лист ЦГ. Бр.* 53/14 и 42/17.

Пресуда ЕСЉП у случају Лопез Рибалда и др. (López Ribalda and others) против Шпаније од 9. јануара 2018. године (поднесак бр. 8567/13).

Пресуда ЕСЉП у случају Копланд (Copland) против Уједињеног Краљевства од 3. априла 2007. године (поднесак бр. 62617/00).

Prof. Željko Mirjanić, LL.D.
Full Professor,
Faculty of Law, University of Banja Luka,
Republika Srpska, Bosnia and Herzegovina

THE USE OF INFORMATION TECHNOLOGIES AND EMPLOYEES' PERSONAL DATA PROTECTION

Summary

Employers use information technologies to collect, process, handle and store employees' personal data, which that are necessary for exercising rights and obligations during the employment relationship, and an employee has a right to protection of data during and after the termination of the employment relationship. In order to guarantee the protection of personal data and privacy of employees, there is a need to give more significance to the legal regulation of the way these technologies are used. Besides the higher risk of abuse of personal data that comes with the use of the technologies and the need to change the legal practice reflected in the fact that employees rarely ever use the right to personal data protection, another important reason for legal regulation is the obligation (stemming from the Stabilization and Association Agreement to gradually align the domestic law with the EU law. These reasons influence the predominant opinion that the national legislation should incorporate the European standards in this area envisaged in Regulation (EU) 2016/679 of the European Parliament and Council of April 2016 concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data. The paper also discusses the influence of information technologies on the protection of personal data of employed "whistle-blowers ".

Keywords: *protection of privacy and personal data of employees, the influence of information technologies on personal data protection, protection of employed whistle-blowers.*