



УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ



Остваривање и заштита права на приватност запослених

(мастер рад)

Ментор
Доц. др Марија Драгићевић Ђорђевић

Студент
Марија Миленковић
Број индекса: M002/23-ИТ

Ниш, 2025

САДРЖАЈ

I УВОД.....	1
II ПРАВО НА ПРИВАТНОСТ	2
III ПРАВО НА ПРИВАТНОСТ ЗАПОСЛЕНИХ.....	6
IV МЕЂУНАРОДНИ СТАНДАРДИ ОД ЗНАЧАЈА ЗА ОСТВАРИВАЊЕ И ЗАШТИТУ ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ.....	7
4.1. Право на приватност запослених у оквиру Организације уједињених нација.	8
4.2. Право на приватност запослених у оквиру Међународне организације рада	10
V СТАНДАРДИ САВЕТА ЕВРОПЕ ОД ЗНАЧАЈА ЗА ОСТВАРИВАЊЕ И ЗАШТИТУ ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ.....	11
VI СТАНДАРДИ ЕВРОПСКЕ УНИЈЕ ОД ЗНАЧАЈА ЗА ОСТВАРИВАЊЕ И ЗАШТИТУ ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ.....	13
VII ОСТВАРИВАЊЕ И ЗАШТИТА ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ У УПОРЕДНОМ ПРАВУ	17
7.1. Право на приватност запослених у Црној Гори	17
7.2. Право на приватност запослених у Босни и Херцеговини.....	22
7.3. Право на приватност запослених у Хрватској.....	25
VIII ОСТВАРИВАЊЕ И ЗАШТИТА ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ У СРБИЈИ	30
8.1. Начела обраде података запослених.....	32
8.1.1. Начело законитости, поштења и транспарентности	33
8.1.2. Начело ограничења у односу на сврху обраде	34
8.1.3. Начело минимизације података	35
8.1.4. Начело тачности	36
8.1.5. Начело ограничења чувања података	37
8.1.6. Начело интегритета и поверљивости	38
8.2. Основ обраде података.....	39
8.3. Право на приватност биометријских података.....	41

8.4. Право на приватност запослених и неке специфичне мере надзора	43
8.4.1. Контрола употребе службених средстава за комуникацију	44
8.4.2. Допуштеност алко-теста и теста на дрогу запослених	45
8.4.3. Видео-надзор запослених у просторијама послодавца.....	48
8.4.4. Контрола кретања запослених путем ГПС-а	51
8.5. Институционални механизми заштите права на приватност запослених и санкције у случају његовог кршења	54
IX ЗАКЉУЧАК.....	56
X ЛИТЕРАТУРА	59
XI ОСТАЛА ИСТРАЖИВАЧКА ГРАЂА.....	62
XII САЖЕТАК И КЉУЧНЕ РЕЧИ	68
XIII ABSTRACT AND KEYWORDS	70
XIV БИОГРАФИЈА СТУДЕНТА.....	72

I УВОД

Право на приватност, које припада корпусу основних људских права, последњих деценија, услед убрзаног развоја технологије постаје све учесталији предмет истраживања правне теорије, али и предмет детаљнијег регулисања од стране надлежних институција.

У савременом добу, под технолошким условима, који су непрестани извор промена, право на приватност изложено је бројним ризицима, али и ограничењима.

У међународном праву усвајају се прописи који настоје да испрате све промене које са собом доноси развој саврмених информационих технологија, како би се пружила адекватна заштита приватности уопште, али и приватности запослених, и на тај начин регулисао супериорнији положај послодавца. Најзначајнији прописи донети су под окриљем Организације уједињених нација и Међународне организације рада.

На простору Европе, питањима остваривања и заштите права на приватност баве се како Савет Европе, тако и Европска унија, која је доношењем Опште уредбе о заштити података о личности у великој мери довела до унификације ове области, будући да су све државе чланице Европске уније имале обавезу да своје националне прописе ускладе са њеном садржином.

Међународне и националне институције имају за циљ превазилажење проблема у погледу успостављања и одржавања равнотеже између оправданих интереса послодавца и заштите фундаменталних права запослених, те тековину њиховог настојања чине савремени међународни и национални прописи, заједно са установљеним стандардима.

Нарочито је значајно питање остваривања и заштите права на приватност у сфери радних односа, где је присутан однос супротстављених интереса послодавца и запосленог, те стога у радним односима остваривање и заштита права на приватност добијају нову димензију. Савремено радно окружење изнедрило је питање постојања и постављања границе између легитимних интереса послодавца и заштите достојанства и основних права запослених, али и постављање границе између пословног и приватног живота запослених.

Мастер рад за предмет има анализу поступка остваривања и заштите права на приватност запослених у радном окружењу, са посебним освртом на изазове које савремене технологије надзора попут система видео-надзора, система ГПС праћења, те електронске контроле комуникације доносе у радноправним односима. Рад се базира на

анализи међународних и европских стандарда, упоредноправних решења, са посебним акцентом на домаћу регулативу и правне институте и решења, за која се определио законодавац, са освртом на праксу релевантних органа.

Научни циљ рада је пружање систематичног приказа и критичке анализе права на приватност запослених, кроз преглед теоријских концепата, међународних, регионалних и националних нормативних извора, као и релевантне судске праксе. Посебна пажња усмерена је на упоредноправну анализу. Циљ је и да се утврди у којој мери постојећа нормативна решења одговарају на изазове савременог доба. Прагматични циљ рада огледа се у идентификовању кључних изазова који се јављају у пракси у вези са остваривањем и заштитом права на приватност запослених, као и у предлагању могућих решења ради унапређења постојеће регулативе и праксе. Посебан значај придаје се анализи улоге и праксе Повереника за информације од јавног значаја и заштиту података о личности, као органа надлежног за заштиту овог права у домаћој пракси.

Мастер рад посвећен је и анализи упоредноправних института и нормативних решења, те је стога обрађена заштита приватности запослених на примеру нормативног оквира и праксе надлежних органа Црне Горе, Босне и Херцеговине и Хрватске.

Највише пажње посвећено је домаћој регулативи, у којој кровни пропис у овој области представља Закон о заштити података о личности, који, уз бројне недостатке који доводе до озбиљних разматрања, на теоријском и практичном нивоу, регулише заштиту података о личности на један општи начин, уз домаћај у области рада и запошљавања. Доношењем овог закона домаћа правна регулатива у одређеној мери усклађена је са правом Европске уније, тачније са Општом уредбом о заштити података о личности, међутим присутне су и даље одређене разлике, као и децидно неуређене области, као што су регулисање обраде биометријских података и вршење видео-надзора. Такође, изостављено је и регулисање питања (не)допуштености алко-теста и теста на дрогу запослених, којима се задире у приватност запослених и нарушава заштита података о личности.

II ПРАВО НА ПРИВАТНОСТ

Дефинисање права на приватност се мењало кроз историју и различите историјске, политичке и правне оквири, међутим његов значај у данашњем друштву је остао подједнако важан, може се рећи чак и већи имајући у виду технолошки развој,

који је довео и доводи до стварања многобројних начина задирања у право на приватност. Захваљујући технолошком развоју, право на приватност постаје једно од најосетљивијих права појединаца.

Приватност, као централни сегмент права на приватност, није универзално прихваћен правни појам, већ је подложен различитим тумачењима. Приликом његовог одређења постоје варијације у складу са индивидуалном перцепцијом појединаца, специфичностима социолошког, културолошког и правног концепта, те личним карактеристикама лица на које се то право односи, стога одређивање приватности захтева комплексан и интердисциплинарни приступ.

Приватност су разноразне информације на темељу којих се може штошта закључити (Dragičević Prtenjača, Zagorec, 2023: 58). Односно, приватност се односи на она права која су везана за личност човека и предмете који су непосредно везани за њу (Димитријевић, 2011: 199). Приватност једног лица подразумева подручје које није јавно, везује се за саму особу, те подручје у ком се не предузимају радње у име власти, послодавца итд. (Trifunović, 2019: 66). Приватност се може дефинисати као способност индивидуе или пак групе да друге лиши информација (Sućeska, Hanić, 2014: 626).

Како наводи судија Весна Трифуновић у својој стручној анализи, појмом приватност је обухваћено више сфера човековог живота и то: интимна (којој нико нема приступ), приватна (којој приступ има породица, укућани, доктори, адвокати и др.) и приватно – јавна (која представља приватан живот појединца, али се реализује на јавном простору). Према другом схватању, могуће је класификовати четири основне врсте приватности: одбрамбену приватност, приватност људских права, личну приватност и контекстуалну приватност. (Allen, 2015).

Најједноставније одређивање права на приватност је право да се буде остављен на миру (Warren, Brandeis, 1890: 193). Овакво одређење права на приватност представља једну од првих, модерних дефиниција приватности у правном смислу. Право на приватност представља апсолутно право које поједницу гарантује интегритет и дигнитет људске личности у циљу очувања тајности и слободе приватног живота (Димитријевић, 2011: 203). Може се одредити као право физичког лица, апсолутног и субјективног карактера, да самостално одлучи о упознавању трећих лица са било којом манифестацијом своје егзистеније (Синђелић, 2012: 9). Дакле, појединац сам одлучује о томе који подаци ће бити задржани у његовој приватној сфери, а које ће поделити са другима и на тај начин изаћи из домена приватности. Право на приватност престаје

објављивањем чињеница од стране самог појединца или уз његов пристанак (Warren, Brandeis, 1890: 218). У питању је право појединца, групе, односно институција да сами за себе одреде када, како, али и у којој мери ће се другим лицима саопштавати информације о њему (Westin, 1967: 7).

Право на приватност чине четири права: право на поштовање приватног живота, право на поштовање породичног живота, право на поштовање дома и право на поштовање преписке (Димитријевић, Пауновић, Ђерић, 1997: 283-284). Право на приватност уско је повезано са правом на заштиту података о личности, односно у питању су два неистоветна права, која се истовремено прожимају, стога један од најважнијих аспеката остваривања приватности у савременом добу јесте заштита података о личности. Право заштите података о личности представља битан елемент сваког од горе наведених права, док истовремено представља и самостално, независно право, јер заштита података о личности представља полазну основу заштите ових права (Гасми, Прља, 2020: 7). Заједничка природа ова два права није уочена само у доктрини и њиховим теоријским одређењима, већ и у судској пракси, односно у начину поимања њихове суштине у сваком конкретно случају. Међусобна веза примећена је и у пракси судова Европске уније, из које се може закључити да прави разлику између наведених права, међутим не прави суштинске и значајне дистинкције у погледу дефинисања и примене (Лазовић, 2023: 225). У том смислу, наведена права се схватају као различити правни институти, чија је срж заштита истих интереса, те се сходно томе јавља узорочно – последична веза између истих, будући да се нелегитимним задирањем у личне податке појединца нужно доводи до нарушавање права на приватност. Наиме, међусобна блиска повезаност права на приватност и права на заштиту података о личности произилази из немогућности остваривања наведених права без њихове међусобне повезаности (Гасми, Прља, 2020: 14).

За јасније разумевање института заштите података о личности неопходно је пре свега одредити и дефинисати појам податка, али и синтагму лични податак. Податак потиче од латинске речи „*datum*“ и на нашем језику се може превести као „нешто што је дато“ (Андоновић, Прља, 2020: 9). Податак обично представља знакове, обрасце, карактере или симболе који потенцијално представљају процес или објекат из стварног света (Bygrave, 2010: 14) Податак се одређује као симбол у облику слова и бројева, аналогне или дигиталне слике или звука, који се могу преносити и интерпретирати било од стране људи или уз помоћ аутоматизованог система. То су чињенице о некоме или нечему (Андоновић, Прља, 2020: 9). Податак о личности представља сваку

информацију која се односи на физичко лице које се у неком тренутку може идентификовати (Krivokapić et al. 2016: 13). Дакле, подаци се могу одредити као лични подаци уколико се могу повезати са конкретним појединцем (Станковић, 2016: 7).

У доктрини се право на личне податке одређује и као овлашћење да лице само одлучује о давању, али и обради личних података, без обзира на степен поверљивости тих података (Гајин et al. 2005: 69-70). Право на заштиту података о личности обухвата све врсте података о личности које могу бити предмет обраде података о личности, без обзира на обим утицаја на приватан живот појединца (Гасми, Прља, 2020: 11). Реч је о сложенем праву, из којег произилази низ различитих овлашћења, која законодавци кроз различите законе, уредбе и регулативе гарантују. У питању су овлашћења у вези са избором начина прикупљања, обраде, чувања, мењања и брисања података о личности. Развој савремених информационих технологија омогућио је да се пренос и интерпретација података о личности могу чинити на бржи и ефикаснији начин, али уједно и угрозио њихову сигурност.

Право на приватност, које долази из каталога основних људских права, јесте универзално право, које је загарантовано међународним, регионалним и националним прописима. Универзална декларација о правима човека¹ на међународном плану предвиђа да се нико не сме изложити произвољном мешању у приватни живот, породицу, стан или преписку, нити нападима на част и углед. Свако има право на заштиту закона против оваквог мешања или напада.² Затим је право на приватност потврђено Међународним пактом о грађанским и политичким правима³ и Међународним пактом о економским, социјалним и културним правима⁴.

На простору Европе усвојена је Европска конвенција за заштиту људских права и основних слобода⁵ која гарантује да свако има право на поштовање свог приватног и породичног живота, дома и преписке.⁶

У светлу динамичног технолошког напретка и изненадних и непредвидивих промена које доносе нове изазове, свако одређење права на приватност и права на

¹ Универзална декларација о правима човека (Universal Declaration of Human Rights, Adopted by General Assembly resolution 217/III, 10.12.1948, Paris).

² Ibid., чл. 12.

³ Међународни пакт о грађанским и политичким правима (*Службени лист СФРЈ – Међународни уговори и други споразуми*, бр. 7/71).

⁴ Међународни пакт о економским, социјалним и културним правима (*Службени лист СФРЈ – Међународни уговори и други споразуми*, бр. 7/71).

⁵ Европска конвенција о заштити људских права и основних слобода (*Службени гласник Србије и Црне Горе - Међународни уговори*, бр. 9/03).

⁶ Ibid., чл. 8.

заштиту личних података мора бити конципирано тако да задржи своју применљивост и релевантност кроз време, обезбеђујући при томе ефикасну заштиту праву, упркос потенцијалним технолошким и друштвеним трансформацијама.

Због своје специфичне природе, радни однос угрожава сигурност права на приватност запослених и често доводи до нарушавања истог, будући да је реч о супротстављеним интересима учесника радноправног односа.

III ПРАВО НА ПРИВАТНОСТ ЗАПОСЛЕНИХ

Радноправни однос се заснива закључивањем уговора о раду и нужно подразумева стављање на располагање послодавцу великог броја личних података запосленог. Уговор о раду је *intuitu personae* уговор, односно реч је о уговору који се закључује између тачно одређених лица, при чему је лично својство једне стране одлучујући фактор за закључење. Овакав правни однос послодавца и запосленог указује да послодавац често располаже великим бројем података о запосленом, које потенцијално може искористити против њега и тиме му проузроковати како материјалну, тако и нематеријалну штету.

Док право на приватност обухвата право да се буде остављен на миру, радни однос даје послодавцу право да не остави раднике на миру (Hendrickx, 2020: 8). Стога је неопходно пружити адекватну законску заштиту запосленима, будући да је реч о лицима која се налазе у подређеном положају у односу на послодавце. Наиме, послодавци често имају моћ у односу на запослене имајући у виду њихов однос субординације и често злоупотребљавају своја овлашћења у вези са прикупљањем, обрадом и коришћењем података о личности не само запослених, већ и кандидата за запослење. Са друге стране послодавцима су неопходни подаци ради обезбеђивања безбедности и здравља на раду, испуњавања других обавеза, као и заштите својих легитимних интереса (Ковачевић, 2021: 964). Сходно томе, на страни послодаваца постоји дужност вођења евиденција о запосленима, које обухватају личне податке истих, а све у циљу несметаног обављања делатности послодавца и остваривања низа радних, али и социјалних права запослених (Рељановић, 2020: 63). Питање права запослених у погледу заштите личних података односе се на све информације које послодавац може пронаћи о запосленом (Vasiljković, 2019: 41). Дакле, неопходно је наћи равнотежу и правно уредити однос запосленог и послодавца на начин који ће бити

повољан по запосленог, а са друге стране неће утицати на легитимне интересе послодавца. Разумевање граница легитимног задирања у приватност и механизма правне заштите од кључног је значаја за очување приватности у радном односу. У радноправном односу исправно је прикупљање само неопходне количине информације, уз јасно одређење периода чувања истих и прикупљања информација само за одређену сврху, без употребе у друге сврхе, осим на основу пристанка запосленог (Miller, Weckert, 2000: 258).

Право на приватност припада и кандидатима у процесу запошљавања. Будући да се и кандидати налазе у подређеном положају, имајући у виду њихову потребу за заснивањем радног односа, ова категорија лица поред чињенице да не може значајно да утиче на услове закључења уговора о раду, не може ефективно да утиче ни у погледу обима и врсте података који се прикупљају приликом спровођења конкурса и процеса запошљавања (Vasiljković, 2019: 30). Прикупљени подаци приликом селекције кандидата могу да открију информације о потенцијалним запосленима, које могу значајно да утичу на избор послодавца. Тако, сазнања послодавца о породичном статусу кандидаткиње⁷ могу утицати да послодавац закључи како су кандидат и/или кандидаткиња другачијег породичног статуса адекватнији избор. Задирање у приватност апликаната неретко може имати дискриминаторне последице, те је нужно ограничити и свести на најнижи ниво овакве поступке. Имајући у виду наведене околности на страни законодавца је обавеза успостављања императивних законских норми, ради заштите подређене стране у радном, али и потенцијалном радном односу.

IV МЕЂУНАРОДНИ СТАНДАРДИ ОД ЗНАЧАЈА ЗА ОСТВАРИВАЊЕ И ЗАШТИТУ ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ

Савремени радни односи постављају озбиљне изазове у погледу очувања и остваривања права на приватност запослених, нарочито услед убрзаног технолошког напретка и неједнаког положаја страна у радном односу. Због ових изазова, од круцијалног значаја по приватност запослених је утврђивање јасних граница легитимног обрађивања личних података и обезбеђивање ефикасних механизма правне

⁷ Термин кандидаткиња употребљен је ради указивања на специфичне ситуације у којима се жене приликом запошљавања могу наћи, будући да су у пракси често изложене питањима којима се свесно задира у њихову приватност, попут планирања породице и трудноће, о чему ће касије бити више речи.

заштите истих. Управо у том контексту значајно место припада међународноправним актима, који постављају универзалне стандарде заштите приватности. На глобалном нивоу, међународно право, нарочито кроз систем Уједињених нација и Међународне организације рада утврђује и препоручује принципе који државама чланицама служе као темељ за уређивање права на приватност у радним односима.

4.1. Право на приватност запослених у оквиру Организације уједињених нација

Организација уједињених нација, као кровна међународна организација, има развијен систем прописа и стандарда којима се регулише остваривање и заштита права запослених, укључујући и право на приватност запослених. Наиме, Универзална декларација о правима човека експлицитно предвиђа заштиту права на приватност тако што наводи да се нико не сме изложити произвољном мешању у приватни живот, породицу, стан или преписку, нити нападима на част и углед. Свако има право на заштиту закона против оваквог мешања или напада.⁸ Стога је право на приватност како негативног карактера, јер државе или други актери треба да се уздрже од мешања у приватност било ког човека, тако и позитивног карактера, јер свако има право на адекватне мере које обезбеђују заштиту од таквог мешања у његову приватност (Maschlanka, 2017: 26). Иако Универзална декларација о правима човека на експлицитан начин штити право на приватност, изостављене су одредбе које директно штите право на приватност запослених, стога се заштита запослених остварује кроз наведени члан. Универзална декларација о правима човека јесте необавезујућег, декларативног карактера, али, без обзира на то, представља темељ заштите људских права свих држава потписница.

Исти модел заштите права на приватност прати и Међународни пакт о грађанским и политичким правима који у члану 17. прокламује право на приватност и заштиту овог права.⁹ Међутим, за разлику од Универзалне декларације о правима човека, Међународни пакт о о грађанским и политичким правима је обавезујућег карактера, будући да се свака држава чланица овог Пакта обавезује да поштује и обезбеди свим лица која се налазе на њеној територији и под њеном надлежношћу права призната у овом Пакту, без икакве разлике, као што је раса, боја коже, пол, језик, вера, политичко или друго мишљење, национално или социјално порекло, имовинско

⁸ Чл. 12. Универзалне декларације о људским правима.

⁹ Чл. 7. Међународног пакта о грађанским и политичким правима.

стање, рођење или други статус.¹⁰ Комитет за људска права УН, чији је задатак надгледање примене овог Пакта, у свом општем коментару бр. 16 Пакта о грађанским и политичким правима наводи: Члан 17 (Право на приватност) усвојен на 32. седници Комитета за људска права указује да државе имају обавезу како да се уздрже од произвољног мешања у приватност, тако и да предузму све неопходне позитивне мере, како би се спречило мешање трећих лица у приватни живот појединца, а то чине обезбеђењем ефикасног законодавног оквира, који таква дела забрањује и физичким и правним лицима.¹¹ У контексту радних односа ово значи да је неопходно да државе потписнице успоставе законодавне и институционалне механизме којима ће обезбедити да послодавци поштују границе приватности својих запослених, нарочито водећи рачуна о прикупљању, чувању и обради података о личности, надзору запослених, тестирању и другим поступцима који могу нарушити приватну сферу запослених.

Међународни пакт о економским, социјалним и културним правима својим одредбама не гарантује експлицитно право на приватност, међутим гарантује да свако лице има право да се користи правичним и повољним условима за рад.¹²

Под окриљем Организације уједињених нација 1990. године усвојене су и Смернице за регулисање компјутеризованих база података о личности¹³, које штите податке о личности. Смерницама за регулисање компјутеризованих база података о личности су усвојени Правични принципи који се односе на обраду података о личности, као и препоруке које се односе на усвајање националних смерница, оне регулишу и ограничење Правичних принципа, ако постоји потреба заштите људских права појединаца, или у циљу остваривања хуманитарне помоћи (Станковић, 2016: 12). Смернице за регулисање компјутеризованих база података о личности предвиђају предузимање одговарајућих мера ради заштите фајлова, како од природних опасности, као што су случајни губитак или уништење, тако и од људских опасности, као што су неовлашћени приступ, злоупотреба података или заражавање компјутерским

¹⁰ *Ibid.*, чл. 2.

¹¹ Општи коментар бр. 16 Пакта о грађанским и политичким правима: Члан 17 (Право на приватност) Право на поштовање приватности, породице, дома и преписке, као и заштиту части и угледа (*CPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation Adopted at the Thirty-second Session of the Human Rights Committee, New York, April 1988*).

¹² Чл. 7. Међународног пакт о економским, социјалним и културним правима.

¹³ Смернице за регулисање компјутеризованих база података о личности (*Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95, New York, December 1990*).

вирусима.¹⁴ На овај начин државе су обавезане да обезбеде одговарајући правни оквир којим се ограничава и санкционише евентуално прекорачење овлашћења послодавца и на тај начин спречава задирање у приватност запослених.

4.2. Право на приватност запослених у оквиру Међународне организације рада

Међународна организација рада, која ствара међународне радне стандарде и принципе у међусобним односима између послодаваца и запослених, поставља стандарде и у вези са заштитом приватности запослених. На Састанку стручњака о приватности радника усвојен је Кодекс праксе о заштити личних података радника¹⁵ који је објављен 1997. године. У Преамбули Кодекса наведено је да различити системи надзора и контроле личних података доводе до стварања потребе за развојем посебних правила којима се регулише заштита личних података запослених, а као разлог истакнута је заштита достојанства радника, заштита приватности и права на то да запослени сами одлуче ко ће користити њихове податке, у које сврхе и под којим условима ће се то чинити.¹⁶ Циљ Кодекса је да пружи опште смернице за заштиту података запослених.¹⁷ Лични подаци се дефинишу као информације које идентификују или могу идентификовати запосленог.¹⁸ Сходно Кодексу сваки запослени располаже правом да ужива право на приватност, те стога запослени може бити заштићен од било каквих мера надзора, уколико послодавац не оправда потребу за ограничењем тог права (Maschlanka, 2017: 26).

Поред Кодекса праксе о заштити личних података радника, Међународна организација рада је разматрала и друге аспекте радне средине који се везују за приватност на радном месту. Као резултат дискусије на састанку експерата у Женеви 1996. године усвојен је Кодекс праксе о управљању питањима везаним за алкохол и дроге на радном месту.¹⁹ Као додатак V уз Кодекс праксе о управљању питањима везаним за алкохол и дроге на радном месту приложено је Упутство за тестирање на

¹⁴ *Ibid.*, 2.

¹⁵ Кодекс праксе о заштити личних података радника (*Protection of workers' personal data*. An ILO code of practice, International Labour Office, Geneva, 1997).

¹⁶ *Ibid.*, 1.

¹⁷ *Ibid.*

¹⁸ *Ibid.*

¹⁹ Кодекс праксе о управљању питањима везаним за алкохол и дроге на радном месту (*Management of alcohol – and drug – related issues in the workplace*. An ILO code of practice, International Labour Office Geneva, 1996).

дрогe и алкохол на радном месту²⁰, које је усвојено на Саветовању у Ослу 1993. године. Једно од питања о ком је било речи јесте и које законске, етичке и моралне стандарде треба применити приликом спровођења програма тестирања на дроге, као и како постићи равнотежу између индивидуалних права запослених и права послодавца.²¹

Наведени документи уз основне принципе које дефинише Међународна организација рада представљају основу развоја националних прописа држава чланица Међународне организације рада, који имају за циљ регулисање радноправног окружења, заштиту права запослених и гарантовање овлашћења послодаваца.

V СТАНДАРДИ САВЕТА ЕВРОПЕ ОД ЗНАЧАЈА ЗА ОСТВАРИВАЊЕ И ЗАШТИТУ ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ

Европска конвенција о људским правима прокламује право на поштовање приватног и породичог живота, дома и преписке²², које према ставу Европског суда за људска права, обухвата и активности професионалне и пословне природе.²³ Овако прописан чл. 8. Европске конвенције о људским правима представља основу за доношење низа прописа и препорука у оквиру Савета Европе у области заштите приватности запослених. Једнако значајна је и пракса Европског суда за људска права, који доношењем пресуда штити ово фундаментално право.

У сфери запошљавања, Комитет Министара Савета Европе настоји да прилагоди и уподоби заштиту права на приватност радном окружењу. На тај начин пружа адекватну заштиту запосленима, али и уважава права и дужности послодаваца, све у циљу остваривања њихових легитимних интереса. Комитет Министара Савета Европе усвојио је Препоруку број Р(89)2 о заштити личних података коришћених у сврхе запошљавања²⁴, а затим и Препоруку CM/Rec(2015)5²⁵ о обради личних података у

²⁰ Упутство за тестирање на дроге и алкохол на радном месту (*Guiding principles on drug and alcohol testing in the workplace as*, Adopted by the ILO Interregional Tripartite Experts Meeting on Drug and Alcohol Testing in the Workplace, Oslo, May 1993).

²¹ *Ibid.*, 4.

²² Чл. 8. ст. 1. Европске конвенције за заштиту људских права и основних слобода.

²³ Препорука CM/Rec(2015)5 Комитета министара државама чланицама о обради личних података у контексту запошљавања (Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, Adopted by the Committee of Ministers at the 1224th meeting of the Ministers' Deputies (Brussels, April 2015)).

²⁴ Препорука број Р(89)2 о заштити личних података коришћених у сврхе запошљавања (Recommendation No. R (89) 2 of the Committee of Ministers to member States on the processing of personal data used for employment purposes, Adopted by the Committee of Ministers at the 423rd meeting of the Ministers' Deputies (Strasbourg, January 1989)).

контексту запошљавања. Разлог за доношење Препоруке CM/Rec(2015)5 о обради личних података у контексту запошљавања су промене које су се догодиле у области запошљавања, а нарочито напредак у развоју информационо-комуникационих технологија и обухвата заштиту података како у приватном, тако и у јавном сектору.²⁶

Поред тога што Европски суд за људска права у својим пресудама успоставља опште стандарде очувања права на приватност, он је такође донео и бројне, значајне пресуде које се односе на приватност у радном окружењу. Тако створена пракса Европског суда за људска права је изузетно одговорима на питања која за предмет имају различите сфере приватности запослених. Пресудом *Halford v. the United Kingdom*²⁷ Суд је одлучио да пресретање телефонских позива запослене, од стране послодаваца, из пословних просторија представља угрожавање приватног живота и преписке и да је на тај начин дошло до повреде члана 8. Европске конвенције о основним правима. Пресудом *Copland v. the United Kingdom*²⁸ Европски суд за људска права је утврдио да задирање у личне информације запослене које се тичу телефона, као и електронске поште и интернета, без њеног знања, представља задирање у њену приватност, у смислу члана 8. Европске конвенције о основним правима. Суд је такође утврдио да подносиатељка представке није добила од стране послодавца упозорење да се њене позиви могу надзирати, те је сходно томе разумно очекивала приватност позива које је упућивала са пословног броја, а исто је могла очекивати и за коришћење порука путем електронске поште и коришћење интернета. Подносиатељка представке је истакла да је послодавац могао интреним актима упознати запослене са политиком у вези праћења коришћења телефона и других средстава комуникације, што послодавац није учинио. Значајна је и Пресуда *Barbulescu v. Romania*²⁹ у којој је Суд нашао да послодавац својим поступцима не може у потпуности да задире у личне податке запосленог, без обзира на своја упутства дата запосленима. Чињеница да је запослени био свестан да постоји забрана коришћења интернета у приватне сврхе, не значи да је запослени обавештен и о могућности, као и обиму надзора над преписком запосленог

²⁵ Препорука број CM/REC (2015)5 о обради личних података у контексту запошљавања (Recommendation CM/Rec(2015) of the Committee of Ministers to member States on the processing of personal data in the context of employment, Adopted by the Committee of Ministers on the 1224th meeting of the Ministers' Deputies (Strasbourg, April 2015)).

²⁶ *Ibid.*, 1.

²⁷ Case ECHR of *Halford v. The United Kingdom*, Appl. No. 20605/92, од 25.06.1997. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-58039%22%5D%7D>, преузето 14.09.2024. године.

²⁸ Case ECHR of *Copland v. the United Kingdom*, Appl. No. 62617/00 од 03.04.2007. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22002-2765%22%5D%7D>, преузето 14.09.2024. године.

²⁹ Case ECHR of *Bărbulescu v. Romania*, Appl. No. 61496/08, од 05.09.2017. <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-177082%22%5D%7D>, преузето 14.09.2024. године.

од стране послодавца. Пресудом *Niemitz v. Germany* Европски суд за људска права закључио је да поштовање приватног живота мора у одређеној мери укључивати и право на успостављање и развијање односа са другим, односно није могуће јасно разликовање које активности запосленог чине део његовог професионалног или пословног живота, а које то не чине.³⁰ Европски суд за људска права донео је пресуду у погледу кршења права на приватност запослених од стране послодавца и у случају који се водио против Црне Горе. Наиме, Пресудом *Antović and Mirković v. Montenegro*³¹ суд је истакао да приватност може укључивати и професионални живот појединца. Суд је истако да видео-надзор запосленог на радном месту представља значајно ометање приватног живота запосленог. Пресудом *Fernández Martínez v. Spain*³² Европски суд за људска права утврдио је да је професионални живот запосленог део његовог приватног живота.

VI СТАНДАРДИ ЕВРОПСКЕ УНИЈЕ ОД ЗНАЧАЈА ЗА ОСТВАРИВАЊЕ И ЗАШТИТУ ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ

Право на приватност представља једно од основних људских права зајемчених у правном поретку Европске уније. Повељом Европске уније о основним правима³³ из 2000. године загарантовано је право на поштовање приватног и породичног живота, дома и комуникације³⁴, чиме је успостављен темељ заштите права на приватност. Наведени документ отишао је корак даље у развоју концепта приватности и прокламовао право на заштиту података о личности као посебно, самостално право. На овај начин је, по први пут, на простору Европске уније право на заштиту података о личности прокламовано као самостално право. Иако Повеља испрва није имала обавезујући карактер, ступањем на снагу Лисабонског уговора од 2009. године³⁵ добила је обавезујући карактер. Значај Повеље се огледа у чињеници да је на простору Европске уније то први правни акт који је издвојио право на заштиту података о

³⁰ Case ECHR of *Niemitz v. Germany*, Appl. No. 13710/88 од 16.12.1992. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-57887%22%5D%7D>, преузето 14.09.2024.

³¹ Case ECHR of *Antović and Mirković v. Montenegro*, Appl. No. 70838/13 од 28.11.2017. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-178904%22%5D%7D>, преузето 05.09.2025. године.

³² Case ECHR of *Fernández Martínez v. Spain*, Appl. No. 56030/07 од 12.06.2014. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-145068%22%5D%7D>, преузето 15.08.2025. године.

³³ Повеља Европске уније о основним правима (Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, C 364/1).

³⁴ *Ibid.*, чл. 7.

³⁵ Лисабонски уговор (Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, *Official Journal of the European Communities*, C 306/1).

личности из корпуса права на приватност и сврстао га у ред фундаменталних права човека. Члан 8. Повеље Европске уније о основним правима прокламује да свако има право на заштиту података о својој личности, а затим и предвиђа да се подаци морају обрађивати поштено, за одређену сврху и на основу информисаног пристанка особе или на неком другом легитимном основу уређеном законом.³⁶ Иако Повеља не садржи одредбе које изричито уређују право запослених на приватност и заштиту података о личности, чланом 31. прописује право на правичне и поштене услове рада, који подразумевају да свако има право на услове рада којима се не нарушавају здравље, безбедност и достојанство. Индиректно на овај начин, заштићено је право на приватност и право на заштиту података о личности у радном окружењу.

У циљу пружања свеобухватне заштите података о личности на територији Европске уније, приступљено је изради уредбе која детаљно уређује ова питања. У периоду од 2012. до 2016. године вршено је усаглашавање коначне верзије текста новог прописа, који је имао за циљ усклађивање заштите података о личности у свим државама чланицама Европске уније. *General Data Protection Regulation*, односно Општа уредба о заштити података о личности усвојена је 2016. године, а ступила на снагу 2018. године, државе чланице добиле су рок од 2 године да своје, домаће прописе ускладе са њеном садржином.

Општа уредба о заштити података о личности постала је својеврсни стандард у овој области, будући да је велики број земаља усагласио своје домаће прописе управо са Општом уредбом о заштити података, због избегавања строгих казни које прописује (Гасми, Прља, 2020: 12). Један од примера јесте и домаћи Закон о заштити података о личности, који заправо представља у већој мери преведен и прилагођен текст Опште уредбе о заштити података о личности (Тошић, Новаковић, 2020: 94). Доношењем Опште уредбе о заштити података о личности послодавци су обавезани да се придржавају њених норми у радном односу који постоји према запосленима. На овај начин пружена је заштита запосленима и омогућено им је остваривање једног од фундаменталних права. У Преамбули Опште уредбе о заштити података о личности прописано је да се могу доносити посебна правила о обради података о личности запослених. Члан 88. предвиђа да државе чланице могу утврдити прецизнија правила обраде података запослених, која укључују прикладне и посебне мере за заштиту

³⁶ Чл. 8. Повеље Европске уније о основним правима уније о основним правима.

људског достојанства.³⁷ Суд правде Европске уније у предмету *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v. Minister des Hessischen Kultusministeriums*³⁸ утврдио је да државе чланице могу, али и не морају да утврђују прецизнија правила, те да она могу бити садржана у закону или колективном уговору. Даље је Суд правде утврдио да је слобода државе чланице приликом употребе ове одступајуће клаузуле маргинаилована, будући да слободу доношења закона морају користити у складу са условима и ограничењима одредама Опште уредбе о заштити података о личности и да приликом доношења прописа не могу доводити у питање њен садржај и циљеве.

Радна група из члана 29. у својим мишљењима даје допринос тумачењу норми европског права и правилној примени истих, давањем смерница и мишљења. Мишљење 2/17 о обради података на радном месту³⁹ представља допуну раније донетих публикација Радне групе из члана 29. – Мишљења 8/2001 о обради личних података у контексту запослења⁴⁰ и Радног документа о надзору електронских комуникација на радном месту⁴¹. Мишљење 2/17 о обради података на радном месту даје смернице у погледу тумачења Опште уредбе о заштити података о личности, истиче новине које доноси у контексту запослења. Члан 25. Опште уредбе о заштити података о личности⁴² предвиђа да је руковалац приликом обраде података дужан да предузме све одговарајуће техничке и организационе мере, што би према смерници Радне групе значило да је послодавац дужан да примени решења која у највећој мери штите податке о личности запослених када послодавци запосленима дају на коришћење уређаје⁴³. Занимљиво је и схватање Радне групе да послодавци не би требало да захтевају од запослених приступ њиховим личним профилима на друштвеним мрежама.⁴⁴

Европски одбор за заштиту података основан је чланом 68. Опште уредбе о заштити података о личности, са задатком да обезбеђује доследну примену уредбе, у

³⁷ Чл. 88. Опште уредбе о заштити података о личности.

³⁸ Case European Court of Justice of *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v. Minister des Hessischen Kultusministeriums*, C-34/21 од 30.03.2023. [CURIA - Documents](#), преузето 17.08.2025. године.

³⁹ Мишљење 2/17 о обради података на радном месту (Opinion 2/2017 on data processing at work, Adopted by Article Data Protection Working Party (Brussels, June 2017)).

⁴⁰ Мишљење 8/2001 о обради личних података у контексту запослења (Opinion 8/2001 on the processing of personal data in the employment context, Adopted by Article 29 Data Protection Working Party (Brussels, September 2001)).

⁴¹ Радни документ о надзору електронских комуникација на радном месту (Working document on the surveillance of electronic communications in the workplace, Adopted by Article 29 Data Protection Working Party (Brussels, May 2002)).

⁴² Чл. 25. Опште уредбе о заштити података о личности.

⁴³ Мишљење 2/17 о обради података на радном месту, 8.

⁴⁴ *Ibid.*, 13.

погледу пружања општих смерница, одлучује о доследној примени у конкретном случају, даје мишљена Европској комисији итд.⁴⁵ Европски одбор за заштиту података осврнуо се на личне податке запослених у Смерницама 07/2020 о појмовима руковоаца и обрађивача података у Општој уредби о заштити података о личности⁴⁶. У Смерници је утврђено да се под појмом лица која су овлашћена за обраду података о личности под непосредним надлежношћу руковоаца или обрађивача⁴⁷ подразумева упућивање на лица која припадају руковоацу или обрађивачу података, као правном лицу, у смислу запосленог, али и лица која се са руковацем или обрађивачем налазе у односу који је сличан радном односу, али само у мери у којој су овлашћени да обрађују податке.⁴⁸ Дакле, запослени, или лице изједначено са њим, које изађе из граница постављених овлашћења и приступи подацима у сврху различиту од сврхе послодавца, сматраће се „трећим лицем“. Сходно томе сносиће све последице и преузеће одговорност која се односи на обраду података о личности. Дакле, уколико запослени врши обраду података о личности запослених код послодавца, на начин којим прекорачава дата овлашћења и супротно сврси, запослени који врши обраду биће одговоран због злоупотребе личних података запослених код послодавца.

Институционални механизам заштите права на приватност запослених у Европској унији чини Суд правде Европске уније. Основна овлашћења Суда правде Европске уније састоје се у тумачењу уговора, у смислу својеврсних устава и вршењу судске контроле над законима и праксом држава чланица (Garrett et al. 1998: 149). Пракса Суда правде Европске уније има посебан значај, будући да су одлуке суда обавезујућег карактера за државе чланице, што представља гаранцију јединствене примене права у свим националним системима. Управо због тог обавезујућег карактера пракса чини драгоцен извор тумачења права генерално, а нарочито у погледу заштите права на приватност запослених, где је често потребно прецизирање и тумачење правних стандарда. У случају C-579/21⁴⁹ пред Суд правде Европске уније разматрано је

⁴⁵ Чл. 70. Опште уредбе о заштити података о личности.

⁴⁶ Смернице 07/2020 о појмовима руковоаца и обрађивача података у Општој уредби о заштити података о личности (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Adopted by European Data Protection Board (Brussels, September 2020)).

⁴⁷ Реч о лицима која не представљају „треће лице“ у складу са чл. 4. ст. 1. тач. 10. Опште уредбе о заштити података о личности.

⁴⁸ Смернице 07/2020 о појмовима руковоаца и обрађивача података у Општој уредби о заштити података о личности, 29.

⁴⁹ Case European Court of Justice of J.M. v. Pankki S. C-579/21 од 22.06.2023. <https://curia.europa.eu/juris/document/document.jsf?jsessionid=854390868FA9C07247E123379BA74EA2?text=&docid=274867&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=21943358>, преузето 17.08.2025. године.

да ли запослени J.M. у банци *Pankki S*, чији је истовремено био и клијент, има право да потражује, између осталог и информације које се тичу идентитета лица, које под руководством послодавца и његовим упуштвима, врши увид у личне податке запосленог. Суд правде стао је на становиште да, сходно Општој уредби о заштити података о личности, послодавац нема обавезу да на захтев запосленог открије информације о идентитету запосленог који је под његовим упутством и руководством вршио обраду, већ да то може учинити искључиво ако су те информације неопходне како би се остварило ефикасно остваривање права зајемчених уредбом, а све у складу са узимањем у обзир и права и слобода тих запослених.

VII ОСТВАРИВАЊЕ И ЗАШТИТА ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ У УПОРЕДНОМ ПРАВУ

Прописи који се усвајају и на међународном и на регионалном нивоу доприносе унификацији заштите података о личности запослених, међутим без обзира на то, свакако су присутне значајне разлике између различитих правних система.

7.1. Право на приватност запослених у Црној Гори

Правни оквир који регулише право на приватност запослених у Црној Гори у великој мери одражава решења усвојена у правном систему Републике Србије, будући да се ради о државама које повезује вишедеценијско постојање унутар јединственог државног апарата и јединственог правног система.

Уставом Црне Горе⁵⁰ јемчи се неповредивост физичког и психичког интегритета човека, његове приватности и личних права.⁵¹ Овако зајемчено право на приватност обухвата право на поштовање приватног и породичног живота.⁵² Такође, Устав гарантује и заштиту података о личности запослених, на уопштен начин, забрањује њихову употребу ван намене за коју су прикупљени, прописује да свако лице има право да буде упознато са подацима који су прикупљени о његовој личности, а гарантује и судску заштиту у случају злоупотребе.⁵³ На овај начин се на уопштен начин регулише заштита права на приватност и заштита података о личности, без осврта на приватност

⁵⁰ Устав Црне Горе, *Сл. лист ЦГ*, 01/07.

⁵¹ *Ibid.*, чл. 28.

⁵² *Ibid.*, чл. 40.

⁵³ *Ibid.*, чл. 43.

запослених.

Закон о раду Црне Горе⁵⁴ експлицитно прописује дужност послодаваца да поштују личност запослених, штите њихову приватност и обезбеђују заштиту личних података запослених.⁵⁵ Овако постављеном одредбом законодавца, директно је зајемчена заштита приватности запослених.

На уопштен начин, правила о заштити података о личности запослених доноси и Закон о заштити података о личности⁵⁶ од 2020. године. У Црној Гори подаци о личности запослених штите се под условима и на начин прописан Законом о заштити података о личности, а све у складу са принципима и стандардима потврђених међународним уговорима и општеприхваћеним правилима међународног права.⁵⁷ Лични подаци представљају све информације о физичком лицу чији идентитет је утврђен или се може утврдити,⁵⁸ док су посебне категорије личних података они подаци који се односе на расно или етничко порекло, политичко мишљење, затим верско или филозофско уверење чланство у синдикалним организацијама, као и подаци у вези са здравственим стањем или сексуалним животом.⁵⁹ Задирање у приватност запослених обрадом личних података могуће је под условом да постоји сагласност запосленог или у случају да не постоји сагласност, ако је обрада неопходна ради извршавања законом прописаних обавеза, заштите живота и других виталних интереса лица које не може сагласност да да лично, ради извршења уговора, обављања послова од јавног интереса или вршења јавних овлашћења и остваривања законом предвиђеног интереса.⁶⁰ Законодавац Црне Горе дозвољава обраду посебних података о личности запослених између осталог уз изричиту сагласност или ако је обрада неопходна ради заснивања радног односа, а у складу са законом којим се уређују радни односи, уз обавезно поштовање адекватних мера заштите.⁶¹

У погледу посебне категорије личних података који се односе на здравствено стање лица⁶² према Закону о здравственој заштити ужива се право на приватност и поверљивост свих података који се односе на здравље лица.⁶³ Прописано је да су сви

⁵⁴ Закон о раду Црне Горе, *Сл. лист ЦГ*, 49/2008.

⁵⁵ *Ibid.*, чл. 19. ст. 1. тач. 10.

⁵⁶ Закон о заштити података о личности, *Сл. лист ЦГ*, 79/08.

⁵⁷ *Ibid.*, чл. 1.

⁵⁸ *Ibid.*, чл. 9. ст. 1. тач. 1.

⁵⁹ *Ibid.*, тач. 7.

⁶⁰ *Ibid.*, чл. 10. ст. 1. и ст. 2.

⁶¹ *Ibid.*, чл. 13. ст. 1. тач. 1. и 2.

⁶² *Ibid.*, чл. 9 ст. 1. тач. 7.

⁶³ Закон о здравственој заштити, *Сл. лист ЦГ*, 8/21.

учесници у пружању здравствене заштите дужни да воде одговарајућу медицинску документацију, затим да се прописани подаци воде за пацијенте у папирној или електронској форми, да су извор података за збирке података у складу са методологијом вођења и управљања збиркама података, у складу са посебним законом.⁶⁴ Врста и садржај медицинске документације, начин и поступак вођења, овлашћена лица за вођење и унос података, рокови достављања и обраде података, начин располагања подацима као и друга питања везана за вођење медицинске документациј уређени су посебним законом.⁶⁵ Сви посебни подаци о личности који се односе на здравствено стање запослених, морају се обрађивати у складу са наведеним правним нормама.

Начин поступања са личним подацима који спадају у посебну категорију личних података регулисан је и Правилником о начину означавања и заштите посебних категорија личних података⁶⁶. Правилник је донет од стране Министарства унутрашњих послова Црне Горе, а објављен 18.02.2011. године. Прописано је да приликом обраде личних података у које спада и посебна категорија личних података државни орган, орган државне управе, орган локалне самоуправе и локалне управе, привредно друштво и друго правно лице, предузетник и физичко лице, а које има седиште, односно пребивалиште на територији Црне Горе и врши обраду личних података, успостављање збирке личних података на начин и за намену утврђену законом или његовим актом мора свим фазама обраде означити да се ради о обради личних података који спадају у посебну категорију.⁶⁷ Када се послодавци нађу као руковоаци подацима означавање наведене категорије података мора извршити стављањем ознаке „Посебна категорија личних података“.⁶⁸ Послодавци су дужни, да кад се јаве као руковаци збирке личних података, донесу план заштите посебне категорије личних података и да уједно обезбеде организационе, техничке и кадровске мере заштите података, као и да обезбеде спровођење тих мера.⁶⁹ Датим Правилником законодавац је прописао на који начин се означава и штити посебна категорија личних података, што је од значаја за запослене, будући да послодавци често располажу штићеним подацима.

⁶⁴ *Ibid.*, чл. 135. ст. 1. и ст. 2.

⁶⁵ *Ibid.*, чл. 135. ст. 3.

⁶⁶ Правилник о начину означавања и заштите посебних категорија личних података, *Сл. лист ЦГ*, 011/11.

⁶⁷ *Ibid.*, чл. 3. ст. 1.

⁶⁸ *Ibid.*, чл. 3. ст. 2.

⁶⁹ *Ibid.*, чл. 4.

Значајну улогу у праћењу примене прописа и унапређења заштите података у Црној Гори има Агенција за заштиту података и слободан приступ информацијама, која је основана Законом о заштити података о личности.⁷⁰ Агенција путем својих мишљења и препорука указује на правилну примену закона у пракси, укључујући и ситуације у радним односима. Као резултат свог деловоња доноси препоруке, савете и мишљења. Агенција је обрадила питање надзора запослених и као резултат свог става донела Савет *Употреба глобалног позиционог система – ГПС у сврхе праћења службених возила, Обавезе руковоца и права лица чији се подаци обрађују* од 29.04.2025. године. Према ставу Агенције запослени који користи службена средства за рад, чије се употреба прати путем ГПС уређаја мора бити на адекватан начин упознат са сврхом обраде, начином коришћења података, обавезама и правима и интерним правилима којима је уређена ова материја. Када је реч о приватним возилима, која се користе у службене сврхе и том приликом прате преко ГПС уређаја, неопходно је да се употреба истог ограничи искључиво на радно време запосленог, тачније време обављања радних задатака, уз претхонду писану сагласност запосленог. (*Upotreba globalnog pozicionog sistema – GPS u svrhe praćenja službenih vozila, Obaveze rukovaoca i prava lica čiji se podaci obrađuju* од 29.04.2025. године). Послодавац је дужан да предузме одговарајуће мере како би се праћење базирало искључиво на пословну сферу кретања запосленог. На овај начин обезбеђује се заштита приватног живота запосленог.

Значајна разлика између Закона о заштити података о личности Црне Горе и Закона о заштити података о личности Републике Србије је у погледу регулисања видео-надзора. Наиме, у домаћем законодавству изостављене су одредбе којима би се регулисао видео-надзор, док у црногорском законодавству видео-надзор је регулисан чак и у погледу права и дужности запослених и послодаваца. Послодавац може вршити видео-надзор приступа службеним или пословним просторијама, у циљу безбедности лица и имовине, контроле уласка или изласка из наведених просторија, или уколико због природе посла постоји могући ризик за запослене⁷¹, као и због заштите безбедности лица или имовине или тајних података и пословних тајни, а које се не могу остварити на други начин.⁷² Једна од обавеза послодавца је да запослене који раде под видео-надзором у писаном облику обавести о вршењу ове врсте надзора.⁷³ Поред тога неопходно је да послодавац обезбеди да сам систем видео-надзора буде заштићен од

⁷⁰ Чл. 50. Закона о заштити података о личности.

⁷¹ *Ibid.*, чл. 35. ст. 1.

⁷² *Ibid.*, чл. 36. ст. 1.

⁷³ *Ibid.*, чл. 35. ст. 5.

неовлашћеног приступа⁷⁴ и да се лични подаци запослених прикупљени путем видео-надзора не чувају дуже од шест месеци⁷⁵, чиме се гарантује остваривање начела интегритета и начела ограниченог чувања података о личности прикупљених на овај начин. Законодавац забрањује постављање система видео-надзора запослених у просторијама ван радног места, нарочито у гардеробама, лифтовима и санитарним просторијама, али и у простору предвиђеном за странке и посетиоце.⁷⁶ Појам приватног живота обухвата активности и у пословној и у професионалној сфери, те постављање система видео-надзора у просторијама које послодавци користе за одмор и рекреацију у току дневног рада, али и за пресвлачење, представља значајан упад у приватну сферу запосленог и неоправдано задирање у приватност запосленог.⁷⁷ Постављање видео-надзора противно прописима представља повреду права на приватности, док чињеница да снимци начињени том приликом нису објављени не представља услов за повреду приватности, као права личности и за остваривање накнаде штете по том основу.⁷⁸ Дакле, повреда права на приватност постоји без обзира на даљи начин поступања послодавца са снимцима, у погледу њиховог даљег коришћења и објављивања.

Право на приватност може бити ограничено правом на слободан приступ информацијама од јавног значаја. Закон о слободном приступу информацијама од јавног значаја предвиђа да орган власти може приступити информацији или делу информације, уколико је то у интересу заштите приватности од обелодањивања података предвиђених законом којим се уређује заштита података о личности, осим у случајевима када се подаци односе на јавне функционере, у вези са вршењем јавне функције, као и на приходе, имовину и сукоб интереса тих лица и њихових сродника.⁷⁹ На овај начин приступа информацијама од јавног значаја на уштрб приватности и заштити података о личности, како функционера, тако и њихових сродника који су обухваћени законом.⁸⁰ Сходно наведеном подаци о уплаћеним порезима на доходак физичког лица, који је остварен по основу личних примања, као и подаци о називу уплатиоца пореза не чине податке о личности који се штите сходно Закону о заштити

⁷⁴ *Ibid.*, чл. 39. ст. 5.

⁷⁵ *Ibid.*, чл. 37. ст. 3.

⁷⁶ *Ibid.*, чл. 36. ст. 2.

⁷⁷ Пресуда Вишег суда у Подгорици, Гж. 3730/23 од 23.11.2023. године, <https://pn2.propisi.net/?di=sp75816&dt=sp&dl=75816>, преузето 18.06.2025. године.

⁷⁸ Пресуда Вишег суда у Подгорици, Гж. 1542/24 од 15.05.2024. године, <https://pn2.propisi.net/?di=sp79577&dt=sp&dl=79577>, преузето 18.06.2025. године.

⁷⁹ Чл. 14. ст. 1. тач. 1. Закона о слободном приступу информацијама од јавног значаја, *Сл. лист ЦГ*, 30/17.

⁸⁰ Чл. 15. ст. 4. Закона о пореској администрацији, *Сл. лист ЦГ*, 52/19.

података о личности, већ информације од јавног значаја.⁸¹ Насупрот наведеном, оценом Суда, одбици од зараде запослених, по основу плаћања чланарине политичким партијама, су подаци који се не могу учинити доступним као информације од јавног значаја, будући да податке о политичком мишљењу представљају посебне категорије личних података, сходно чл. 9. ст. 1. тач. 7. Закона о заштити података о личности.⁸²

7.2. Право на приватност запослених у Босни и Херцеговини

Систем заштите права на приватност у Босни и Херцеговини одступао је од система заштите у Републици Србији све до марта 2025. године, када је ступио на снагу нови Закон о заштити личних података,⁸³ чијим одредбама је извршено усклађивање заштите личних података са системом Европске уније, а посредно и системима државама које нису чланице Европске уније, али су своје правне системе заштите уподобиле систему Европске уније.

Устав Босне и Херцеговине⁸⁴ гарантује право на приватни и породични живот, дом и преписку.⁸⁵ Устав Босне и Херцеговине не јемчи посебно право на заштиту личних података, нити предвиђа посебну заштиту права на приватност запослених. Насупрот томе Закон о раду Босне и Херцеговине⁸⁶ на уопштен начин регулише поступање са личним подацима запослених и прописује да се лични подаци запослених не могу прикупљати, обрађивати и користити, односно достављати трећим лицима, осим у случају када је то одређено законом или је потребно ради остваривања права и обавеза и радног односа.⁸⁷ Законом о раду у институцијама Босне и Херцеговине⁸⁸ као посебним законом, јемчи се да се лични подаци запослених не могу прикупљати, користити, нити достављати трећим лицима, осим када је то одређено законом или уколико је неопходно како би се остварила права и обавезе из радног односа.⁸⁹ Истим законом право на приватност запослених штите се забраном послодавцу да приликом закључења уговора о раду не могу од запосленог тражити податке који нису у вези са

⁸¹ Пресуда Управног суда Црне Горе, У. 363/23 од 19.09.2023. године, <https://pn2.propisi.net/?di=sp74937&dt=sp&dl=74937>, преузето 18.06.2025. године.

⁸² Пресуда Управног суда Црне Горе, У. 1792/17 од 26.02.2018. године, <https://pn2.propisi.net/?di=sp54995&dt=sp&dl=54995>, преузето 18.06.2025. године.

⁸³ Закон o zaštiti ličnih podataka, *Sl. glasnik BiH*, 12/2025.

⁸⁴ Ustav Bosne i Hercegovine, *Sl. Glasnik BiH*, 25/2009.

⁸⁵ *Ibid.*, чл. 2. ст. 3.

⁸⁶ Закон o radu Bosne i Hercegovine, *Sl. novine FBiH*, 39/2024.

⁸⁷ *Ibid.*, чл. 30.

⁸⁸ Закон o radu u institucijama Bosne i Hercegovine, *Sl. glasnik BiH*, 88/2023.

⁸⁹ *Ibid.*, чл. 15.

природом радних активности које би запослени требао обављати.⁹⁰ Посебно се прописује забрана послодавцу да од жене која се пријавила на расписани јавни оглас послодавца или је већ запослена, тражи да уради тест за утврђивање трудноће.⁹¹

Надаље се заштита личних података запослених уређује Законом о заштити личних података. Нови Закон о заштити личних података резултат је дугогодишњих напора да се правни оквир приватности и заштите података модернизује и приближи европским стандардима (Letica, 2025). Законодавац лични податак одређује као сваки податак који се односи на физичко лице чији је идентитет утврђен или се може утврдити.⁹² Закон о заштити личних података се посебно осврће на обраду личних података у контексту запослења. Прописано је да се посебним законом или колективним уговором прецизирају правила у циљу осигуравања заштите права и слобода у вези са обрадом личних података у контексту запослења, а нарочито за потребе запослења, извршења уговора о раду, укључујући и извршавање обавеза прописаних законом или колективним уговором, затим за потребе управљања, планирања и организације рада, једнакости, али и различитости на радном месту, здравства и сигурности на раду, потом заштите имовине, за потребе остваривања и уживања права и погодности из радног односа, и наравно за потребе престанка радног односа.⁹³ Правила одређена законом обухватају мере заштите људског достојанства носиоца података, његових легитимних интереса и остваривања права, а све нарочито у вези са транспарентношћу обраде, преносом личних података унутар групе привредних субјеката, или групе привредних субјеката који обављају заједничку привредну делатности, као и надзором на радном месту.⁹⁴ Овако формулисаном одредбом успостављена је обавеза, усмерена изричито на послодавце, предузимања одговарајућих мера ради заштите личних података запослених и тако пружена правна заштита права на приватност на терену радних односа. Регулисање права на заштиту личних података запослених представља новину у односу на претходни Закон о заштити личних података⁹⁵, који се овим питањем није бавио непосредно. Још једна новина коју доноси Закон је питање обраде биометријских података у службеним просторијама. За разлику од Закона о заштити личних података из 2011. године који биометријске податке само сврстава у посебну категорију података, без њиховог даљег одређења, нови Закон

⁹⁰ *Ibid.*, чл. 14. ст. 1.

⁹¹ *Ibid.*, чл. 14. ст. 2.

⁹² Чл. 4. ст. 1. тач. 1. Закона о заштити личних података.

⁹³ *Ibid.*, чл. 55. ст. 1.

⁹⁴ *Ibid.*, чл. 55. ст. 2.

⁹⁵ Закон о заштити личних података, *Sl. glasnik BiH*, 89/2011.

дефинише биометријски податак као лични податак који је добијем посебном техником обраде у вези са физичким особинама, затим физиолошким обележјима или обележјима понашања физичког лица која омогућавају или потврђују јединствену идентификацију тог лица, попут фотографија лица и дактилопских података.⁹⁶ Затим, посебну пажњу заслужује чл. 57б. Закона, који се односи на обраду биометријских података запослених у службеним просторијама. Наиме, законодавац допушта обраду ових података у сврху евидентирања радног времена, као и ради контроле уласка и изласка из службених просторија, под условом да је таква одредба прописана законом или се спроводи као алтернатива другим решењима за евиденцију. Међутим у оба случаја неопходно је да запослени да изричиту сагласност за обраду, у складу са одредбама закона којим се уређује заштита података о личности.⁹⁷

Начин чувања и технике заштите личних података уређени су Правилником о начину чувања и посебним мерама техничке заштите личних података,⁹⁸ који је Вијеће министара Босне и Херцеговине донело 02.07.2009. године. Правилником су ближе уређени начин чувања и мере техничке заштите личних података. Под начином чувања заштићених података се подразумева предузимање организационих и техничких мера заштите, као и сачињавање плана сигурности личних података.⁹⁹ Организационим мерама се, у складу са Правилником, подразумевају: информисање и обука запослених који раде на обради личних података, физичке мере заштите радних просторија и опреме у којима се врши обрада, потом спречавање неовлашћеног умножавања, копирање и преписивања лични података и друго.¹⁰⁰ Техничке мере подразумевају контролу приступа просторијама и опреми за обраду личних података, али и заштиту од уништења и оштећења личних података.¹⁰¹ Будући да је Правилник донет у складу са Законом о заштити података о личности Босне и Херцеговине који штити личне податке и запослених, његове одредбе обавезујуће су и за послодавце који обрађују личне податке.

Послодавци могу обрађивати податке о личности, као и у земљама у окружењу, на основу сагласности запосленог или на основу закона.¹⁰² Онда када је основ за обраду

⁹⁶ Чл. 4. ст. 1. тач. 17. Закона о заштити личних података.

⁹⁷ *Ibid.*, чл. 57б.

⁹⁸ Правилник о начину чувања и посебним мјерама техничке заштите личних података, *Sl. glasnik BiH*, 67/09.

⁹⁹ *Ibid.*, чл. 3.

¹⁰⁰ *Ibid.*, чл. 4. ст. 1.

¹⁰¹ *Ibid.*, чл. 5. ст. 3.

¹⁰² Чл. 8. ст. 1. Закона о заштити личних података.

података сагласност носиоца податка, контролор мора обезбедити доказ да је носилац да сагласност.¹⁰³ Прописано је и под којим условима се даје писана сагласност носиоца података. Уколико се обрада заснива на сагласности која је дата у писаној изјави, а изјава се односи и на друга питања, захтев за сагласност мора бити формулисан на начин да се јасно разликује од других постављених питања, у разумљивој форми и лако доступном облику, те написана јасним и једноставним језиком.¹⁰⁴ Овако одређење предвиђа могућност да се сагласност да у писаној форми и услове под којим то може бити учињено, али не предвиђа законску обавезу. Носиоцу података чији се подаци обрађују на основу дате сагласности остављена је могућност повлачења дате сагласности. Повлачење сагласности се може учинити у било ком тренутку, носилац податка мора бити поучен о том праву пре давања сагласности, а повлачење се мора вршити на једноставан начин, као и давање.¹⁰⁵

Закон о заштити личних података осврће се и на видео-надзор, али не регулише употребу истог у оној мери у којој то чини законодавац Црне Горе. Дозовљен је надгледање одређеног простора видео-назором, под условом да је исто неопходно ради заштите лица и имовине и уколико не преовладају интереси носиоца података.¹⁰⁶ У погледу обима видео-надзора постављен је услов.¹⁰⁷ Послодавци морају, у том смислу, ограничити употребу видео-надзора само на радни простор или део радног простора који је суштини неопходан за постизање заштите лица и имовине. Законом није прописана обавеза писменог обавештавања о вршењу видео-надзора, као што је то, примера ради, случај у законодавству Црне Горе, већ је потребно само да контролор, у овом случају, послодавац, истакне на видном месту ознаку о вршењу видео-надзора.¹⁰⁸

Остаје да време покаже у којој мери ће постојећа легислатива бити усклађена са новим законским оквиром, као и да ли ће предвиђени институти бити применљиви у правном систему Босне и Херцеговинне и омогућити ефикасније остваривање и заштиту права на приватност запослених.

7.3. Право на приватност запослених у Хрватској

Република Хрватска, као чланица Европске уније од 1. јула 2013. године, дужна

¹⁰³ *Ibid.*, чл. 9. ст. 1.

¹⁰⁴ *Ibid.*, чл. 9. ст. 2.

¹⁰⁵ *Ibid.*, чл. 9. ст. 3.

¹⁰⁶ *Ibid.*, чл. 57. ст. 1.

¹⁰⁷ *Ibid.*, чл. 57. ст. 2.

¹⁰⁸ *Ibid.*, чл. 57. ст. 5.

је да своје унутрашње законодавство усклади са правном тековином Уније (*acquis communautaire*), укључујући и прописе који се односе на заштиту личних података и право на приватност. У смислу заштите права на приватност, Република Хрватска примењује Општу уредбу о заштити података о личности. Примена Уредбе остварује се посредством Закона о примени Опште уредбе о заштити података о личности.¹⁰⁹ Право на приватност ужива и уставну заштиту и прокламује се највишим правним актом, Уставом Републике Хрватске.¹¹⁰

Уставом Републике Хрватске штити се поштовање и правна заштита личног и породичног живота.¹¹¹ Гарантована је слобода комуникације као битан елемент права на приватност. Чланом 36. Устава Републике Хрватске загарантована је и неповредива слобода и тајност преписке, као и свих других облика комуникације.¹¹² Законодавац овако постављеном нормом, обезбеђује да се не штити само класична форма комуникације, већ иде корак даље и штити и савремене форме комуникације, попут електронске поште, телефонске разговоре и друге облике. У ком год облику запослени обављали комуникацију, послодавац мора поштовати прописану одредбу. Такође, овако формулисана уставна норма омогућила је заштиту преписке, а уједно и очување права на приватност, чак и у условима савременог технолошког развоја, будући да је општим изразом обухватила и облике комуникације који су се појавили након њеног доношења. Даље, Устав Републике Хрватске сваком појединцу јемчи сигурност и тајност личних података, а њихово прикупљање, обрада и коришћење без пристанка лица могућа је искључиво под условима предвиђеним законом.¹¹³ Устав Републике Хрватске не садржи норме којима се искључиво штити право на приватност запослених, као посебне категорије, већ се на запослене примењују наведене опште одредбе.

Насупрот Уставу Републике Хрватске, Закон о раду Републике Хрватске¹¹⁴ експлицитно предвиђа заштиту приватности радника и уређује начин на који се лични подаци запослених од стране послодаваца могу прикупљати, обрађивати, користити и достављати трећим лицима. Наиме, Закон предвиђа да се наведене радње могу предузимати само уколико је то изричито предвиђено законом или је то неопходно

¹⁰⁹ Zakon o provedbi Opće uredbe o zaštiti podataka Republike Hrvatske, *Narodne novine*, 42/18.

¹¹⁰ Ustav Republike Hrvatske, *Narodne novine*, 5/14.

¹¹¹ *Ibid.*, чл. 35.

¹¹² *Ibid.*, чл. 36. ст. 1.

¹¹³ *Ibid.*, чл. 37.

¹¹⁴ Zakon o radu Republike Hrvatske, *Narodne novine*, 64/23.

ради остваривања права и обавеза из радног односа.¹¹⁵ Уколико послодавци обрађују податке запослених на овак начин, обавезани су да унапред донесу правилник о раду, у којем ће одредити које ће податке обрађивати.¹¹⁶ Закон ограничава ко може вршити обраду података запослених, тако што предвиђа да то могу бити искључиво послодавац или лице које он за то овласти.¹¹⁷ Личне податке запослених не могу обрађивати сва лица, чим се осигурава њихова приватност. На крају, посебно се истиче обавеза тајности. Дакле, свако лице које у обављају својих послова дође у контакт са личним подацима запослених, дужно је да те податке чува као поверљиве.¹¹⁸

Сходно члану 5. ст. 4. Закона о раду Републике Хрватске *ministar rada, mirovinskog sustava, obitelji i socijalne politike* (министар рада, пензијског система, породице и социјалне политике) донео је Правилник о садржају и начину вођења евиденције о радницима и запосленима код послодаваца.¹¹⁹ Правилником се, поред осталог, прописује која лица послодавац мора обухватити евиденцијом, садржај исте, право запослених на приступ евиденцији, обавезе према послодавцима, начин и рок чувања података. Посебно је занимљиво нормативно решење ресорног министра у погледу лица која послодавац мора обухватити евиденцијом. Наиме, послодавци су дужни да у евиденцију уносе податке и о лицима са којима немају закључен уговор о раду. Реч је о лицима која обављају послове на основу других уговора или других прописа, а нарочито лица која се налазе на стручном оспособљавању, којим се не заснива радни однос, студентима, ученицима, деци и малолетним лицима, као и лицима, која у складу са прописима о социјалној заштити или изреченом санкцијом обављају рад у јавном интересу.¹²⁰ Овако широко одређен круг лица, у чију приватност се задире евидентирањем њихових личних података у складу са правилником, довео је до подношења предлога за покретање поступка за оцену сагласности са Уставом Републике Хрватске и Законом о раду Уставном суду Републике Хрватске. Предлагач је у предлогу навео да су одредбе Правилника којим се прописује дужност вођења евиденције о лицима која нису запослена на основу уговора о раду, нису у сагласности са Уставом, као ни са чл. 5. ст. 1. и 4. Закона о раду, на основу којег је Правилник донет. Затим даље наводи да у министар није имао законска овлашћења да утврди

¹¹⁵ *Ibid.*, чл. 29. ст. 1.

¹¹⁶ *Ibid.*, чл. 29. ст. 2.

¹¹⁷ *Ibid.*, чл. 29. ст. 3.

¹¹⁸ *Ibid.*, чл. 29. ст. 7.

¹¹⁹ *Pravilnik o sadržaju i načinu vođenja evidencije o radnicima i zaposlenim kod poslodavaca, Narodne novine*, 55/2024.

¹²⁰ *Ibid.*, чл. 10. ст. 1. тач. 1-6.

овако постављене обавезе, као и да се између осталог нарушава начело пропорционалности, имајући у виду да радно време таквог лица може трајати минимално, нпр. један сат, а да је послодавац дужан да податке о истом у евиденцији чува у наредних шест година. Уставни суд Републике Хрватске није прихватио предлог за оцену сагласности са Уставом и законом. У образложењу је наведено да лица која нису у радном односу на основу уговора о раду могу обављати одређене послове на основу других уговора или посебних прописа. Сврха евидентирања ових лица, како је истакнуто, је стварање услова за правилно и потпуно остваривање права и обавеза из уговора или прописа на основу којих особа обавља рад код послодавца, у складу са Законом о сузбијању непријављеног рада.¹²¹ Међутим, наведена одлука Уставног суда Решење U-II-565/2025 од 20. маја 2025. године¹²² није донета једногласно, већ са два издвојена мишљења. Према првом, законодавна власт је требала да приступи измени и допуни прописа, уколико је постојала потреба за оваком регулативом, како извршна власт не би задржала у овлашћења законодавне власти и тиме нарушила начело поделе власти. У другом издвојеном мишљењу додаје се да кругу лица у чију се приватну сферу задире прикупљањем личних података, нису укључена лица која обављају послова код послодавца на основу уговора о делу, а која чине највећу групу лица која раде код послодавца, али нису уједно и запослени. Истим издвојеним мишљењем сматра се да за одређени круг лица која код послодавца раде, а нису запослена прикупљају подаци, док се за одређени круг лица у истој ситуацији такви подаци не прикупљају, чиме се закључује да овако усвојено решење нема легитимни циљ и да се истим нарушава приватна сфера лица, управо без легитимног циља.

У складу са Законом о примени Опште уредбе о заштити података видео-надзор, као посебни облик надзора над запосленима, се може спроводити само у сврхе које су неопходне и оправдане ради заштиту лица и имовине, под условом да тиме не буду нарушени оправдани интереси лица на која се подаци односе, а који се противе обради личних података путем видео-надзора.¹²³ Обрађивач мора означити да је објект под видео-надзором, а сама ознака мора бити видљива најкасније приликом уласка у подручје које је под видео-надзором.¹²⁴ Поред ових општих услова Закон о примени Опште уредбе о заштити података предвиђа да приликом обраде података о личности

¹²¹ Zakon o suzbijanju neprijavljenog rada, *Narodne novine*, 151/22.

¹²² Rešenje Ustavnog suda Republike Hrvatske U-II-565/2025 од 20. маја 2025. године, <https://www.iusinfo.hr/sudska-praksa/USRH2025B565AII?HighlightQuery=565%2f2025>, преузето 21.06.2025. године.

¹²³ Чл. 26. ст. 1. Zakona o provedbi Opće uredbe o zaštiti podataka Republike Hrvatske.

¹²⁴ *Ibid.*, чл. 27. ст. 1.

запослених морају бити испуњени и услови предвиђени Законом о заштити на раду¹²⁵ сходно члану 30. Послодавцима је дозвољено коришћење надзорних уређаја у сврху контролисање уласка и изласка из радних просторија, ради смањења степена изложености запослених ризику од напада на имовину и физички интегритет и сличних догађаја који могу настати на раду или у вези са радом.¹²⁶ Закон о заштити на раду забрањује коришћење надзорних уређаја у просторијама за личну хигијену и пресвлачење¹²⁷, док Закон о примени Опште уредбе о заштити података забрањује и вршење видео-надзора у просторијама намењеним за одмор запослених.¹²⁸ У односу на земље региона, занимљиво је решење којим законодавац послодавцима коришћење надзорних уређаја, који све време прате кретање радника у току обављања послова, односно уређаја који су постављени тако да су запослени у току читавог радног времена у њиховом подручју, дозвољава само на основу претходно добијене сагласности радничког већа или синдикалног повереника.¹²⁹ У случају изостанка сагласности, послодавцима остаје на располагању могућност да сагласност надомести судска или арбитражна одлука.¹³⁰

Као и у другим земљама, основано је независно тело са задатком да врши надзор над применом прописа који регулишу област заштите података, тело је основано 2004. године под именом Агенција за заштиту особних података. Агенција за заштиту особних података је у смислу члана 51. Опште уредбе о заштити података о личности, остала независни орган који је овлашћен да врши надзор, уз овлашћење да врши надзор и над њеном правилном применом. Агенција, на основу Закона, располаже низом надлежности, те између осталог обавља инспекцијски надзор, уколико је законом прописано покреће и учествује у различитим судским и вансудским поступцима због повреде Уредбе и Закона, овлашћена је да покреће и води поступке против особа које су одговорне због повреде Уредбе и Закона, а поред тога располаже и неким саветодавним овлашћењима (Коваџ, 2019: 6). У свом раду доноси препоруке, мишљења и решења.

Агенција је 21. децембра 2018. године донела Одлуку о успостављању и јавном објављивању пописа врста поступака обраде који подлежу захтеву за процену учиника на заштиту података.

¹²⁵ *Zakon o zaštiti na radu Republike Hrvatske, Narodne novine*, 96/18.

¹²⁶ *Ibid.*, чл. 43. ст. 2.

¹²⁷ *Ibid.*, чл. 43. ст. 3.

¹²⁸ Чл. 30. ст. 2. *Zakona o provedbi Opće uredbe o zaštiti podataka Republike Hrvatske*.

¹²⁹ Чл. 43. ст. 4. *Zakona o zaštiti na radu Republike Hrvatske*.

¹³⁰ *Ibid.*, чл. 43. ст. 5.

VIII ОСТВАРИВАЊЕ И ЗАШТИТА ПРАВА НА ПРИВАТНОСТ ЗАПОСЛЕНИХ У СРБИЈИ

Право на приватност у Републици Србији остварује се и штити не само у оквиру националног правног система, већ и кроз обавезу примене и уважавања међународних стандарда насталих деловањем међународних организација, чије је Србија чланица. Поред тога, иако формално није чланица Европске уније, Србије је у обавези да преузима и примењује и правне тековине Европске уније, будући да се налази у процесу европских интеграција. У том контексту, нормативни оквир заштите и остваривања права на приватност запослених у Србији заснива се на уставним гаранцијама, стандардима ратификованих међународних уговора, законским прописима, као и подзаконским актима којима се ближе уређују поједина питања у вези заштите и остваривања права на приватност.

На уставном нивоу непосредно се гарантује тајност писама и осталих средстава комуникације, а изузеци су дозвољени на основу одлуке суда, ради вођења кривичног поступка или остваривања заштите безбедности Републике Србије, на одређено време и у складу са начином предвиђеним законом.¹³¹ Надаље се јемчи заштита података о личности, тако што се предвиђа да се прикупљање, држање, обрада и коришћење података о личности уређују законом. Забрањена је и кажњива употреба података о личности изван сврхе за коју су прикупљени и свако има право да буде обавештен о прикупљеним подацима, као и право на судску заштиту.¹³² Доношењем Закона о заштити података о личности¹³³ од 2008. године законодавац је приступио подробнијем уређењу ове области. На регионалном нивоу, промене у области остваривања и заштите права на приватност донела је Општа уредба о заштити података о личности.

Након њеног усвајања, ради усаглашавања домаћег законодавства са правним системом Европске уније, у Републици Србији усвојен је 2018. године нови Закон о заштити података о личности у који је заправо имплементирана Општа уредба о заштити података о личности и тзв. Полицијска директива¹³⁴. Иако представља велики корак у развоју заштите података, Закон итекако има недостатака. Највећи проблем

¹³¹ Чл. 41. Устава Републике Србије, *Службени гласник РС*, 98/06.

¹³² Чл. 42. Устава Републике Србије.

¹³³ Закон о заштити података о личности, *Службени гласник РС*, 97/08.

¹³⁴ Полицијска директива (Directive (EU) 2016/680 of the European Parliament and of the Council, *Official Journal of the European Union*, L 119/89, Brussels.)

долази због чињенице да Општа уредба о заштити података о личности садржи Преамбулу од 173 тачака, које нису преведене и имплементирани у закон и на тај начин су бројна питања остала нерегулисана и недефинисана.

Заштита права на приватност запослених у Републици Србији првенствено је регулисана Законом о заштити података о личности, кроз призму заштите личних података, док Закон о раду¹³⁵ садржи само штуре одредбе којима се штити право запослених на приватност, али не и непосредно право на приватност. У складу са чланом 83. Закона о раду нормативно се признаје запосленом искључиво право увида у документе који садрже његове личне податке, уз могућност да тражи брисање истих који нису од непосредног значаја за обављање послова, као и могућност да захтева исправку нетачних података.¹³⁶ На овај начин непосредно је обезбеђен основ активне контроле запосленог над обрадом и чувањем његових личних података, од стране послодавца. Даље, истим чланом прописано је да се трећим лицима не може дозволити приступ личним подацима запосленог, изузев у случајевима који су изричито предвиђени законом или када је такво откривање нужно ради остваривања права и обавеза из радног односа.¹³⁷ Овим се успоставља граница између легитимне потребе послодавца и заштите интереса запослених, односно спречава се произвољно и неосновано дељење личних података са спољним субјектима. У погледу субјекта који могу имати приступ подацима, закон прописује да прикупљање, обрада, употреба и достављање личних података запослених трећим лицима може бити вршено искључиво од стране овлашћеног лица, које именује директор.¹³⁸ Будући да приступ личним подацима запослених могу имати само за то овлашћена лица, омогућена је контрола над обрадом података, али и могућност лакшег утврђивања одговорности у организационој структури послодавца, у случају повреде права на приватност запослених.

Чланом 91. Закона о заштити података о личности¹³⁹ законодавац прописује да се обрада у области рада и запошљавања врши у складу одредба закона којима се уређују рад, запошљавање и колективни уговори, уз примену Закона о заштити података о личности. Поред наведених прописа, тајност електронских комуникација штити и Закон о електронским комуникацијама који забрањује пресретање електронских комуникација

¹³⁵ Закон о раду, *Службени гласник РС*, 95/18.

¹³⁶ *Ibid.*, чл. 83. став 1.

¹³⁷ *Ibid.*, чл. 83. став 2.

¹³⁸ *Ibid.*, чл. 83. став 3.

¹³⁹ Чл. 91. Закона о заштити података о личности.

без пристанка корисника или одлуке суда, на начин предвиђен законом.¹⁴⁰ Сходно наведеној одредби, електронске комуникације запослених су заштићене од неовлашћеног приступа послодаваца, чим се јемчи њихова тајност.

Поред закона, значајну улогу у остваривању заштите запослених у погледу њихових личних података пружају и приручници Повереника за информације од јавног значаја и заштиту података о личности у којима се излажу и став и пракса Повереника, која настаје применом Закона о заштити података о личности. Такође, пре доношења актуелног Закона Повереник је израдио и Модел Закона о заштити података о личности¹⁴¹ од 2017. године, којим је заштиту података о личности ускладио са релевантним европским прописима, будући да је претходни Закон донет пре доношења Опште уредбе о заштити података о личности.

8.1. Начела обраде података запослених

Закон о заштити података о личности прописује начела, којих су обавезни да се придржавају сви руковоаци подацима, укључујући и послодавце, приликом обраде података о личности запослених. Законодавац се определио за таксативно набарајање ових начела, чиме је успостављена *numerus clausus* листа која представља полазну основу за поступање свих субјеката који врше обраду података. Одредба члан 5. Закона о заштити података о личности,¹⁴² којом се уређују основна начела обраде, у значајној мери представља пресликан члан 5. Опште уредбе Европске уније о заштити података,¹⁴³ што указује на тежњу ка усклађивању домаћег правног оквира са основним начелима европског права у овој области.

Како право на приватност у свом ширем смислу обухвата и заштиту личних података, важна улога у његовој заштити припада свакако начелима обраде података. Свако од начела обраде података биће посебно размотрено у наставку с циљем указивања на њихов значај у контексту радноправних односа.

¹⁴⁰ Чл. 126. Закона о електронским комуникацијама, *Службени гласник РС*, 44/10.

¹⁴¹ Модел Закона о заштити података о личности, <https://www.poverenik.rs/sr-yu/%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB-%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%B0-%D0%BE-%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B8-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%B0%D0%BA%D0%B0-%D0%BE-%D0%BB%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D0%B8.html>, преузето 15.09.2024. године.

¹⁴² Чл. 5. Закона о заштити података о личности.

¹⁴³ Чл. 5. Опште уредбе о заштити података о личности.

8.1.1. Начело законитости, поштења и транспарентности

У складу са законском одредбом подаци о личности се морају обрађивати законито, поштено и транспарентно у односу на лице на које се подаци односе, што у контексту запошљавања значи – у односу на запосленог.¹⁴⁴

Законита обрада података подразумева постојање ваљаног правног основа обраде, који се може заснивати на изричитом пристанку запосленог или на одговарајућем законском овлашћењу. Послодавци су дужни да обраду података о личности запослених врше у складу са чланом 12. Закона о заштити података о личности, који таксативно прописује услове под којим се обрада сматра законитом, при чему је довољно да буде исупњен један од алтернативно наведених основа и то: 1) пристанак лица на које се подаци о личности односе на обраду података; 2) уколико је обрада неопходна за извршење уговора или предузимања радњи пре закључења уговора; 3) уколико је неопходно обрада ради поштовања правних обавеза руковооца; 4) уколико је обрада неопходна у циљу заштите животно важних интереса лица о чијим подацима је реч или другог физичког лица; 5) уколико је обрада неопходна ради остваривања јавног интереса и 6) уколико је обрада неопходна ради остваривања легитимних интереса послодавца.¹⁴⁵ „Уколико не постоји изричито законско овлашћење, подаци о личности могу се обрађивати само уз пристанак лица на које се подаци односе“ (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 22).

Начело поштења се односи на савесну обраду података од стране послодавца, а уједно и поштовање права надређености, будући да је реч о неравноправним странама. Неопходно је да послодавци поштено обрађују податке о личности, имајући свест о томе да је реч о туђем личном добром, као и са пуном пажњом и поштовањем. Циљ начела је да повећа свест о значају обраде података о личности (Андоновић, Прља, 2020: 56). Како Повереник за информације од јавног значаја и заштиту података о личности наводи у Приручнику за руковооце, послодавац је, као руковалац, дужан да приликом обраде података да потпуне информације о обради, јер у супротном би

¹⁴⁴ Чл. 5. ст. 1. тач. 1. Закона о заштити података о личности.

¹⁴⁵ *Ibid.*, чл. 12. ст. 1.

давање непотпуних, површних или уопштених информација представљало непоштену обраду података о личности, која се чини са намером да се превари запослени (Повереник за информације од јавног значаја и заштиту података о личности, 2012: 14).

Суштина начела транспарентности огледа се у чињеници да се обрада података не може вршити у тајности, већ је неопходно да се то чини јавно. Дакле, пре обраде података неопходно је да се запосленом омогући да буде упознат са читавим сетом информација и то од стране послодавца, као руковођа, на начин разумљив запосленом (Организација за европску безбедност и сарадњу, Мисија ОЕБС-а у Србији, 2019: 13). На овај начин постиже се правилна информисаност лица запосленог о томе који подаци ће се обрађивати, на који начин и у коју сврху. Нарочито приликом примене одређених мера надзора, пре обраде података, запослени од стране послодавца морају бити унапред обавештени, а пожељно би било и консултовани о примени, разлозима и циљевима њене употребе (Ковачевић, 2010: 18) У Моделу Закона о заштити података о личности начело транспарентности регулисано је самостално и предвиђа да свака информација и комуникација која се односи на обраду мора бити доступна и разумљива сваком, а поред тога и изражена јасним и недвосмисленим језиком.¹⁴⁶ Циљ начела транспарентности је да осигура запосленом да буде упознат са легитимним разлозима ограничења приватности, методима ограничења, трајању и могућим последицама (Ковач Орландић, 2018: 69).

8.1.2. Начело ограничења у односу на сврху обраде

Подаци о личности се прикупљају у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама.¹⁴⁷ Начело сврсисходности према Мишљењу повереника значи да се подаци о личности обрађују у јасно одређену и дозвољену сврху (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 23). Сврха прикупљања података одређује се законским одредбама и свако прикупљање и обрада података супротно законом одређеној сврси је противзаконито. Закон дозвољава даљу обраду прикупљених података, иако нису првобитно прикупљани у ту сврху, уколико је реч о даљој обради у сврхе архивирања у јавном интересу, у сврхе научног или историјског

¹⁴⁶ *Ibid.*, чл. 4.

¹⁴⁷ Чл. 5. ст. 1. тач. 2. Закона о заштити података о личности.

истраживања, као и у статистичке сврхе.¹⁴⁸ Такође, изузетак од правила да се подаци могу обрађивати само у првобитну сврху постоји и у случају прикупљања и обраде података од стране надлежних органа. Наиме, у том случају обрада података која је различита од сврхе за коју су подаци прикупљени, од стране надлежног органа могућа је и уколико су кумулативно испуњена 2 услова, потребно је да је руковалац овлашћен да обрађује те податке у такве друге сврхе и да је обрада сразмерна и неопходна тој другој сврси.¹⁴⁹ Неопходно је да сврха прикупљања података о личности запослених буде експлицитна, конкретно одређена, а сами подаци који се обрађују од стране послодавца морају бити адекватни и релевантни. Сходно томе прикупљање и обрада података о крвној групи запосленог би били оправдани само уколико је реч о пословима у вези којих постоји оправдани ризик у складу са природом посла, на примере уколико је реч о пословима на којима постоји повећани ризик од настанка повреда на раду, у сваком другом случају обрада података не би била у складу са сврхом због које се врши (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 17). Запослени има право да захтева од послодавца информације које се односе на сврху обраде података о личности.¹⁵⁰

8.1.3. Начело минимизације података

Приликом обраде подаци о личности морају бити примерени, битни и ограничени на оно што је неопходно у односу на сврху обраде.¹⁵¹ Свако обрађивање података у мери која је прекомерна у односу на ону која је довољна за постизање сврхе обраде је прекомерна и као таква незаконита, те је стога неопходно вршење минимализације података који се обрађују. „Када обим и врста података нису законом предвиђени, тада руковалац мора, у зависности од ситуације, одлучивати која обрада не представља прекомерну, односно несразмерну обраду података о личности. То подразумева да се у сваком конкретном случају за сваку врсту податка мора преиспитати да ли је обрада тог податка неопходна за остваривање сврхе обраде, а не по инерцији обрађивати податке који у конкретном случају нису уопште потребни.“ (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 23).

¹⁴⁸ *Ibid.*, чл. 6. ст. 1.

¹⁴⁹ *Ibid.*, чл. 7. ст. 1.

¹⁵⁰ *Ibid.*, чл. 29. ст. 1.

¹⁵¹ *Ibid.*, чл. 5. ст. 1. тач. 3.

Обрада ће бити незаконита чак и онда када запослени да сагласност за обраду података, али је сама обрада прекомерена, јер се сврха може остварити и обрадом друге врсте или мањег обима података.

Остваривање исте сврхе обраде података често је могуће достављањем или јавним објављивањем мањег обима података, али је карактеристично да послодавци о томе не воде рачуна, те сходно томе јавно објављују на огласним таблама или достављају другим лицима податке попут ЈМБГ-а запосленог, адресе и других података. Тако је, одговорно лице у правном лицу, прослеђивањем тужби члановима управног одбора, којим су запослени покренули парнични поступак против правног лица поступило супротно начелу минимализације података из члана 5. става 1. тач. 3 Закона о заштити података. Поступања супротног наведеној одредби настало је достављањем неанонимизираних тужби, будући да су нису били заштићени лични подаци и то: име, презиме, адреса становања и ЈМБГ (Повереник за информације од јавног значаја и заштиту података о личности, 2025: 150).

Принцип минимализације података од изузетног значаја је приликом вршења електронског надзора запослених будући да се поставља питање у којој мери могу послодавци вршити електронски надзор над запосленима, имајући у виду природу надзора (Hendrickx, 2022: 27).

8.1.4. Начело тачности

Законодавац је предвидео да је неопходно да подаци који се обрађују буду тачни, а уколико је то потребно и ажурирани, како би обрада података била законита¹⁵², док Модел Закона о заштити података и личности предвиђа да је неопходно да подаци буду поред наведеног и потпуни.¹⁵³ Послодавац је приликом обраде података дужан да води рачуна о исправности података који се обрађују и уколико се јави потреба да изврши измену постојећих, нетачних, односно застарелих података. Потребно је да се предузму неопходне мере како би се омогућила тачност обрађиваних података о личности (Андоновић, Прља, 2020: 69). Закон о раду прописује право запослених да захтевају исправљање нетачних података¹⁵⁴, на овај начин постиже се очување тачности

¹⁵² *Ibid.*, чл. 5. ст. 1. тач. 4.

¹⁵³ Чл. 8. Модела Закона о заштити података о личности.

¹⁵⁴ Чл. 83. Закона о раду.

и ажурности података. С тим у вези, послодавци као руковаоци подацима морају предузети све разумне мере које обезбеђују брисање или исправку нетачних података, без одлагања.¹⁵⁵ Модел Закона о заштити података о личности предвиђа непосредно право лица, чији се подаци обрађују, да захтева од руковаоца да исправи, допуни, ажурира или брише податке о њему који се обрађују, уколико докаже да подаци нису тачни, потпуни, ажурирани, док је руковалац дужан да поступи по захтеву, али и да о извршеним променама обавести све примаоце којима су подаци прослеђени.¹⁵⁶

Са начелом тачности података уско су повезани лични подаци о којима послодавци не могу захтевати одговоре, као што су подаци о породичном односном брачном животу, планирању породице и трудноћи. У вези ових података јавља се тзв. право на лаж запослених (Hendrickx, 2020: 32). На оваква, забрањена питања, запослени или кандидати за запослење, не морају дати одговор, или могу чак дати и погрешне одговоре (Ковачевић, 2021: 974), из чега произилази да овако прикупљени лични подаци, чије прикупљање је забрањено, не подлежу начелу тачности. С тим у вези, Законом о раду послодавцу је забрањено да од кандидата тражи податке о породичном и брачном статусу, као и о плановима у вези са планирањем породице и забрањено је заснивање радног односа тестом трудноће, а једини изузетак од ове забране допуштен је у случају кад је реч о радним местима на којима постоји значајан ризик по здравље жене и детета.¹⁵⁷ У случају када се ради о радним местима на којима постоји ризик, неопходно је поштовање начела тачности и давања тачних информација.

8.1.5. Начело ограничења чувања података

Једно од начела које предвиђа Закон о заштити података о личности јесте начело ограничења чувања података. Овим начелом је утврђено да се подаци чувају само у оном року који је неопходан како би се конкретна сврха обраде података о личности остварила.¹⁵⁸ На тај начин спречава се могућност злоупотребе података, јер се временски оквир чувања података ограничава на најкраћи могући период за остваривање конкретне сврхе. Сходно томе, омогућава се смањивање ризика од злоупотребе података о личности, тако што се ограничава могућност чувања и коришћења туђих података (Андоновић, Прља, 2020: 71).

¹⁵⁵ Чл. 5. ст. 1. тач. 4. Закона о заштити података о личности.

¹⁵⁶ Чл. 51. ст. 1. и ст. 3. Модела Закона о заштити података о личности.

¹⁵⁷ Чл. 26. ст. 2. и ст. 3. Закона о раду.

¹⁵⁸ Чл. 5. ст. 1. тач. 5. Закона о заштити података о личности.

8.1.6. Начело интегритета и поверљивости

Начело интегритета и поверљивости налаже да се подаци морају обрађивати на начин који обезбеђује адекватан ниво заштите, како од незаконите или неовлашћене обраде података, тако и од случајног губитка, уништења или оштећења. Закон прописује да се ова заштита остварује применом одговарајућих мера кадровске, организационе или техничке природе.¹⁵⁹

Када је реч о запосленима, ова одредба подразумева обавезу послодавца да предузме све благовремене и неопходне радње, како би се спречила могућност наношења штете запосленом услед неадекватне заштите података. Мере безбедности које послодавци могу применити, како би поступили у складу са начелом интегритета и поверљивости, у складу са конкретним околностима, укључују: псеудонимизацију и криптозаштиту података; обезбеђивање трајне поверљивости, интегритета, расположивости и отпорности система и услуга обраде; обезбеђивање приступа и расположивости података у случају одређених инцидената, физичке или техничке природе, у најкраћем могућем року и поступак редовног испитивања мера безбедности.¹⁶⁰ Модел Закона о заштити података о личности детаљније уређује мере безбедности и предвиђа да оне нарочито обухватају: заштиту просторија, опреме и системске програмске опреме, заштиту база података и програмских апликација током прослеђивања података, обезбеђење од радњи обраде података, које обухватају и брисање, односно уништавање података и анонимизацију података и обезбеђење могућности да се касније утврди време и место обраде података.¹⁶¹

Правилник о начину претходне провере радњи обраде података о личности¹⁶² предвиђа право Повереника за информације од јавног значаја и заштиту података о личности да врши надзор над спровођењем мера обезбеђења и заштите података, који укучује проверу примене важећих норми, стандарда и техничких упутстава у погледу: прикључења и смештаја рачунара са базама података; обезбеђење уређаја за непрекидно напајање електричном енергијом; заштите модемских прикључака; примене мере обавезног обавештавања руковооца података о свим неовлашћеним

¹⁵⁹ *Ibid.*, чл. 5. ст. 1. тач. 6.

¹⁶⁰ *Ibid.*, чл. 50. ст. 2.

¹⁶¹ Чл. 73. ст. 2. Модела Закона о заштити података о личности.

¹⁶² Правилник о начину претходне провере радњи обраде података о личности, *Службени гласник РС*, број 35/2009.

покушајима приступа подацима; обезбеђење адекватних рачунарских програма и опреме; обезбеђење контроле приступа просторијама у којима се налази рачунарска опрема; примена мера заштите од утицаја свих непогода попут пожара, влаге, хладноће; коришћења одговарајућих пропусница приликом приступа збиркама података и обезбеђивања адекватног потхрањивања података на друге преносице информатичке медије.¹⁶³

У принципу, лични подаци запослених, не могу се учинити доступним трећим лицима, применом наведених одговарајућих мера. Објављивање личних података запослених, попут адресе пребивалишта запосленог или ЈМБГ-а, на огласној табли послодавца представљало би повреду начела интегритета и поверљивости података о личности, будући да се на тај начин изостављају примене одговарајућих мера (Повереник за информације од јавног значаја и заштиту података о личности, 2021: 176).

8.2. Основ обраде података

Обрада података о личности обухвата сваку радњу или скуп радњи које се, аутоматизовано или неаутоматизовано врше над подацима о личности или њиховим скуповима - као што су прикупљање, бележење, разврставање, груписање, односно структурисање, похрањивање, уподобљавање или мењање, откривање, увид, употреба, откривање преносом, односно достављањем, умножавање, ширење или на други начин чињење доступним, упоређивање, ограничавање, брисање или уништавање.¹⁶⁴ Дакле, закон на тај начин предвиђа низ радњи које по својој природи представљају обраду података.

Сагласно Закону о заштити података о личности, ваљан правни основ за обраду личних података може бити закон или пристанак лица она које се подаци односе.¹⁶⁵

Имајући у виду однос субординације између послодавца и запосленог, посебну пажњу захтева питање валидности датог пристанка од стране запосленог. Неретко и запослени и кандидати за запослење, услед страха за свој постојећи/будући радни однос, дају пристанак супротно својој стварној вољи. Отуда се постављање питање: да ли је сваки пристанак на обраду личних података у радном односу или услед заснивања

¹⁶³ *Ibid.*, чл. 9.

¹⁶⁴ Чл. 4. ст. 1. тач. 3. Закона о заштити података о личности.

¹⁶⁵ *Ibid.*, чл. 12.

радног односа законит? Пристанак лица на које се подаци односе мора бити добровољно, одређено, информисано и недвосмислено изражавање воље тог лица, којим запослени, било изјавом или било јасном потврдном радњом даје пристанак за обраду података о личности који се на њега односе.¹⁶⁶ Да би се говорило о ваљаном пристанку, непоходно је да послодавац пристанак прибави складу са чл. 15 Закона о заштити података о личности. Пристанак се не подразумева, већ мора бити дат писмено или усмено на записник. Уколико се пристанак даје приликом давања писане изјаве која садржи и друга питања, захтев за давање изјаве мора бити формулисан на начин који га издваја од других постављених захтева. Захтев мора бити постављен у разумљивом и лако доступном облику, уз употребу једноставног и јасног речника.¹⁶⁷ На овај начин се омогућава запосленом да се недвосмислено упозна са постављеним захтевом и да одговори без довођења у заблуду. Повереник за информације од јавног значаја и заштиту података о личности у одговору број 011-00-00092/2015-05 од 29. јануара 2015. године наглашава да пристанак запосленог мора бити прибављен у складу са начелима сразмерности и сврсисходности (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 21). Дакле, није сваки пристанак запосленог на обраду података о личности истовремено и правноваљан пристанак. Пристанак на обраду података о личности не може бити основ за обраду података о личности уколико запослени може трпети одређене негативне последице услед одсуства пристанка (Ковачевић, 2021: 968). Сматра се да је пристанак за обраду дат слободно, уколико се извршење уговора, као и пружање услуга не условљава давањем оног пристанка који није неопходан за извршење истог.¹⁶⁸

„...Изјава воље мора бити слободно дата, тј. не сме бити дата под претњом, преваром, принудом или у заблуди. Мора бити посебна, тј. дата за тачно одређену сврху и информисана, што значи да лице које даје сагласност има довољно информација које гарантују да оно даје информисани пристанак за обраду својих података. Лице мора да зна ко је руковалац података, које врсте података обрађује, у које сврхе, на који начин ће се подаци користити, колико дуго ће се подаци чувати и друго.“ (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 22). Добровољно дат пристанак запосленог се мора тумачити у духу начела сразмерности и сврсисходности, што значи да иако постоји неспорна сагласност

¹⁶⁶ *Ibid.*, чл. 4. ст. 1. тач. 12.

¹⁶⁷ *Ibid.*, чл. 15. ст. 2.

¹⁶⁸ *Ibid.*, чл. 15. ст. 4.

запосленог да се његови подаци о личности обрађују, обрађивање неће бити законито уколико је обрада несразмерна и несврсисходна. У прилог овоме говори и став Повереника у одговору број: 011-00-00534/2011-05 од 22. новембра 2011. године да није довољно да буде испуњен само услов давања сагласности, већ је неопходно да буде испуњен и услов сразмерности и сврсисходности (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 21).

Запосленом, чији подаци се обрађују, Закон гарантује право да у сваком тренуку могу опозвати престанак који су дали за обраду података, при чему опозив престанка не утиче на радње обраде предузете до тренутка опозива престанка. Послодавци су дужни да запосленог, пре давања престанка обавесте о праву на опозив престанка и о самом дејству опозива.¹⁶⁹

8.3. Право на приватност биометријских података

Развој савремених технологија омогућио је идентификацију појединаца без коришћења традиционалних метода, што је значајно убрзало сам процес идентификације, али је смањило степен заштите приватности запослених. Отвориле су се нове могућности за употребу, али и злоупотребу личних података, што доводи до задирања у приватност појединаца и потенцијалне шете. Један од начина задирања у приватност представља обрада биометријских података физичких лица. Биометрија се одређује као модел идентификације особе, који се базира на физичким карактеристикама или карактеристикама понашања особе (Пауновић et al. 2015: 97). Биометрија као појам подразумева да карактеристике морају бити универзалне, јединствене, непроменљиве, приступачне и мерљиве (Perry R. Cook, 2002).

На домаћем правном плану не постоји посебан пропис који непосредно регулише коришћење биометријских података, те се сходно томе примењују одредбе Закона о заштити података о личности. Овај недостатак правног система Републике Србије, захтева што скорије нормативно уређење. Ипак, законско одређење биометријских података није у потпуности одсутно. Закон о заштити података о личности дефинише биометријске податке као посебну врсту личних података, чија употреба је све учесталија у радним односима. Биометријски подаци представљају личне податке до којих се долази посебном техничком обрадом, а који се односе на

¹⁶⁹ *Ibid.*, чл. 15. ст. 3.

физичка или физиолшка обележја или карактеристике понашања лица и који омогућавају или потврђују јединствену идентификацију физичког лица, попут слике лица или дактилоскопских података.¹⁷⁰

Овакав начин обраде података омогућава послодавцима контролу присуства запослених на радном месту. Међутим, због специфичности биометријских података, није свака обрада таквих података од стране послодаваца законита. За закониту обраду неопходно је постојање пристанка запосленог или другог законитог основа, уз обавезу поштовања основних начела прописаних чл. 5. ст. 1. Закона о заштити података о личности. При томе, код биометријских података само постојање пристанка запосленог на обраду није довољно, неопходно је да поред пристанка буду сагледани и испоштовани и начело сврсисходности и сразмерности.

Закон о раду и Закон о евиденцијама у области рада¹⁷¹ прописују дужност послодавца да води службене евиденције о различитим подацима у вези са радом и запосленима, те сходно томе послодавци настоје да то остварују што ефикасније. Закон о евиденцијама у области рада нарочито прописује обавезу евидентирања података о радном времену запослених и његовом коришћењу.¹⁷² Употреба биометријског софтвера омогућава брзо, прецизно и ефикасно вођење евиденције, међутим ниједан домаћи важећи прописи не дозвољава обраду и коришћење биометријских података, попут снимања отиска прста, без обзира на чињеницу постојања пристанка запосленог, а у сврху прикупљања података о присуству на радном месту. Неспорно је да послодавци имају обавезу прикупљања оваквих података, међутим, дозвољено је прикупљање само оних података који су по броју или по својој врсти сразмерни сврси обраде. Обрада биометријских података у ову сврху сматра се несразмерном, будући да је постизање сврхе могуће и другим средствима, попут постављања лица за контролу присуства, увођењем картица за пријаву и одјаву са радног места и др. Стога, овакав начин обраде није у складу са законским одредбама. Са друге стране, употреба биометријских података може бити оправдана, нарочито када послодавци имају потребу да заштите поједне врсте тајни или процеса рада. Закон о заштити података о личности предвиђа могућност обраде и коришћења биометријских података како би се спречиле потенцијалне штетне последице у вези са радом и омогућила прецизнија контрола на радном месту. Међутим, услови обраде и коришћења биометријских

¹⁷⁰ *Ibid.*, чл. 4. ст. 1. тач. 15.

¹⁷¹ Закон о евиденцијама у области рада, *Службени гласник РС*, 36/09.

¹⁷² Чл. 24. Закона о евиденцијама у области рада.

података су строжи, те стога није дозвољено чување биометријских података запослених, већ се врши њихово накнадно упаривање, тако што се упарују забележени биометријски подаци у одређеном тренутку, са биометријским подацима конкретног запосленог (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 62).

Овакав начин обраде доприноси ефикаснијем спровођењу мера заштите на раду запослених, омогућавајући послодавцима брже и лакше утврђивање ко од запослених је био у одређеном радном простору у тренутку настанка незгоде и пружање правовремене помоћи.

8.4. Право на приватност запослених и неке специфичне мере надзора

Са једне стране, послодавци имају легитимни интерес спречавања ненаменског коришћења радних средстава, као и адекватног обезбеђење радног места која је супротстављена потреби запослених да заштите своју приватну сферу (Драгићевић, 2018: 429). Из тог разлога, надзор који послодавци спроводе над радом запослених и радним просторијама мора бити усклађен са основним начелима заштите приватности запослених.

Надзор над комуникацијом запослених, постављање видео и аудио-надзора, примена ГПС система за праћење и употреба свих других техничких средстава која омогућавају увид у приватност запосленог, захтевају јасно поштовање границе како би се избегло прекомерно задирање у приватност запослених и евентуалне штетне последице. Такве мере морају бити сврсисходне, сразмерне сврси која се њиме жели постићи, и спроведене на начин који не нарушава достојанство запослених.

У бројним правним системима заступљено је становиште да се прекомерним или непотребним надзором запослених крши „обавеза старања“ послодавца о запосленом (Ковач Орландић, 2018: 133). Управо мере као што су видео-надзор, ГПС систем праћења, контрола употребе службених средстава комуникације и друге сличне мере представљају најчешће предмете полемике у теорији и пракси, јер се у њима најдиректније сударају интереси послодаваца и право запослених на приватност.

8.4.1. Контрола употребе службених средстава за комуникацију

Ера информационо-комуникационог напретка ставила је на располагање бројне облике комуникације, које запослени могу користити како у пословне, тако и у приватне сврхе. Под средствима за комуникацију подразумевају се поред телефона и рачунари које запослени користе и средства електронске комуникације попут електронске поште и различитих апликација или друштвених мрежа (Ковач Орландић, 2018: 141). Имајући у виду да је сврха употребе службених средстава за комуникацију везана искључиво за обављање престације рада, законодавац има право како да контролише употребу, тако и да ограничи употребу ових средстава (Драгићевић, 2018: 430). Овакву контролу послодавци могу вршити у циљу спречавања злоупотребе службених средстава за комуникацију, с обзиром на то да постоји дужност запослених да службена средства за комуникацију користе на разуман начин и за законите потребе (Ковачевић, 2014: 339).

Ипак, примена надзора над службеним средствима комуникације отвара бројна питања у вези са правом на приватност. Закон о заштити података о личности не садржи експлицитне норме којима регулише допуштености увида у податке о коришћењу службеног рачунара од стране послодавца, уједно и интернет претраживача, као и приступа електронској пошти запосленог, потом увида у листинг позива и самог службеног телефона.

Употреба службених рачунара је постала уобичајена, будући да престација рада често зависи управо од могућности коришћења рачунара. Врховни касациони суд заузео је став да је опште позната чињеница да многи запослени користе своје службене рачунаре да у њему чувају своје приватне записе¹⁷³, те је у начелу, допуштена употреба службених рачунара у приватне сврхе. Међутим, надзор над електронском поштом и интернет претраживачом запосленог од стране послодавца, аутоматски подразумева и обраду личних података (Žarković, 2015: 175). Већина европских земаља не уређује посебним одредбама питања употребе електронске поште и интернета на радном месту, већ на њих важе општа правила која се односе на заштиту приватног

¹⁷³ Пресуда Врховног касационог суда Србије Рев2 665/2015 од 23.12.2015. године, <https://www.vrh.sud.rs/sr/%D1%80%D0%B5%D0%B22-6652015-%D0%BF%D0%BE%D0%B2%D1%80%D0%B5%D0%B4%D0%B0-%D1%80%D0%B0%D0%B4%D0%BD%D0%B5-%D0%B4%D0%B8%D1%81%D1%86%D0%B8%D0%BF%D0%BB%D0%B8%D0%BD%D0%B5>, преузето 15.09.2024.

живота, а нарочито на заштиту тајности преписке и података о личности (Ковачевић, 2010: 9). Послодавац не треба, осим у изузетним случајевима да проверава приватну електронску пошту запослених, која се налази на приватним налозима запослених, чак и онда кад се са њих обавља пословна преписка, а послодавац се може упознати са њеним садржајем искључиво уколико постоји сагласност запосленог, или без сагласности, али на основу одлуке суда и на одређено време, уколико је неопходно ради вођења кривичног поступка или прикупљања материјалних доказа, или ради заштите безбедности Републике Србије (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 121).

Када је реч о увиду у листинг службених телефонских позива, послодавац такав увид може вршити или на основу пристанка запосленог, или без пристанка запосленог ако за то постоји правни основ. Уколико се лични подаци запослених садржани у листингу позива обрађују на основу сагласности запосленог, она мора бити дата под условима који су прописаним члановима 10. и 15. Закона о заштити података о личности, док уколико је реч о обради која се врши без пристанка запосленог, она се мора вршити сходно члану 12. тачка 3. Закона о заштити података о личности, ако је таква обрада предвиђена уговором о раду закљученог између запосленог и послодавца, у неком општем или у неком појединачном акту послодавца (Повереника за информације од јавног значаја и заштиту података о личности, 2018: 119-120). Сходно томе, обрада података садржаних у листингу позива која се врши супротно наведеним одредбама је незаконита. Послодавац, у начелу, има право, док поступа у границама законских оквира, да приступи пословној, односно службеној преписци запослених, која се одвија преко телефона (Повереник за заштиту података о личности, 2019: 91). Стога, како би се говорило о законитој обради података о личности у погледу приступа информацијама садржаним у службеном телефону запосленог, неопходно је да иста буде у складу са чланом 12. Закона о заштити података о личности.

8.4.2. Допуштеност алко-теста и теста на дрогу запослених

Вршењем алко-теста и теста на дрогу запослених поред напада на приватност запосленог, повређује се и интегритет запосленог, ствара се ризик од дискриминације и повреде достојанства личности, али се и превентивно делује на могуће нежељене последице на раду и штите интереси послодавца (Ковач Орландић, 2018: 181).

Један од легитимних разлога отказа уговора о раду запосленог од стране послодаваца може бити долазак на рад запосленог под дејством алкохола или других опојних средстава, односно употреба алкохола или других опојних средстава у току радног времена, која има или пак може имати утицај на обављање посла.¹⁷⁴ Послодавац не сме да испитује да ли запослени ужива алкохол ван просторија послодавца, или у време одмора, осим онда кад употреба алкохола и ван радног времена утиче на обављање радних обавеза запосленог, на пример у случају професионалних возача (Ковачевић, 2010: 10). Законодавац превиђа да у случају сумње на присуство алкохола или других опојних средстава у крви запосленог, послодавац има могућност да упути запосленог у одговарајућу здравствену установу на анализу, о свом трошку, или да на други начин утврди присуство ових супстанци у крви, у складу са општим актом.¹⁷⁵ Овако прописаном одредбом послодавцима су остављене широке могућности за утврђивање начина тестирања запослених, што они чине доношењем различитих правилника. Законодавац није предвидео количину алкохола у крви запосленог која би утицала или би могла утицати на обављање посла, сходно томе све количине алкохола у крви запослених изнад 0.00 промила могла би представљати разлог за отказ уговора о раду. Разлог отказа уговора о раду може бити и одбијање запосленог да се подвргне тестирању, с обзиром на то да одбијање представља повреду радне дисциплине.¹⁷⁶ У погледу места тестирања интересантан је став Врховног суда по ком је запослени учинио повреду радне дисциплине и радне дужности када је одбио да се уради алко-тест од стране овлашћеног лица послодавца у тренутку када се није налазио на свом радном месту, у канцеларији саобраћајног диспечера, већ у приватном аутомобилу.¹⁷⁷

У пракси, правилници послодаваца којима се одређују услови и начин контроле присуства алкохола предвиђају различите количине алкохола. Тако је Правилником о тестирању запослених у Основном суду у Алексинцу на алкохол и друга средства зависности¹⁷⁸ прописано да се под алкохолисаним стањем запосленог подразумева садржај алкохола у организму већи од 0,30 мг/мл¹⁷⁹, док Правилник о начину и поступку провере алкохолисаности и/или утицаја других опојних средстава запослених

¹⁷⁴ Чл. 179. ст. 3. тач. 4. Закона о раду.

¹⁷⁵ *Ibid.*, чл. 179. став 4.

¹⁷⁶ *Ibid.*, чл. 179. став 5.

¹⁷⁷ Пресуда Врховног суда Србије Рев2 18/07 од 21.02.2007. године, <https://www.vrh.sud.rs/sr-lat/rev2-1807>, преузето 15.09.2024. године.

¹⁷⁸ Правилник о тестирању запослених у Основном суду у Алексинцу на алкохол и друга средства зависности од 19.10.2021. године, Алексинац, [pravilnik o testiranju.pdf \(sud.rs\)](#), преузето 15. 09. 2024. године.

¹⁷⁹ *Ibid.*, чл. 3.

у Градској управи града Прокупља¹⁸⁰ предвиђа да се под алкохолисаним стањем сматра присуство алкохола у крви у већој вредности од 0,00%.¹⁸¹ Поред количине алкохола која је потреба како би се сматрало да се запослени налази у алкохолисаном стању, правилницима се предвиђа и начин и поступак провере присуства алкохола у организму, као и других психоактивних супстанци. Са већим или мањим разликама које постоје међу њима, један од највећих заједничких недостатака правилника ове врсте је нерегулисање заштите приватности запослених. Наиме, иако правилници регулишу ко може вршити проверу, на који начин, под којим условима, они не предвиђају начин штитите података добијених утврђивањем присуства алкохола или других опојних средстава у организму, коме ће смети запослени који врше проверу да саопште добијене податке, затим не регулишу потребу заштите података добијених у здравственим установама приликом алко-теста и теста на дрогу. Узимањем телесних узорак запослених долази се до података о здрављу, у питању су подаци о физичком или менталном здрављу лица, узимајући у обзир и оне податке о пружању здравствених услуга, којима се долази до сазнања о здравственом стању лица.¹⁸² Будући да се обрада података о здравственом стању лица сврстава у обраду посебних података о личности забрањена је од стране послодаваца.¹⁸³ Изузетно, обрада оваквих података послодавцима је дозвољена уколико је неопходна ради процене радне способности запослених, док лице које врши обраду има обавезу чувања података као професионалне тајне.¹⁸⁴ Стога, потребно је да законодавац непосредно регулише употребу теста на алкохол и теста на друге психоактивне супстанце, дужности и права запослених, али и послодаваца приликом тестирања, као и услове под којима ће се вршити тестирање, задирањем у што мањој мери у приватност запосленог. Поред тога, послодавци приликом доношења правилника, такође морају регулисати питање заштите добијених података, који се уско везују за личност запослених.

Заштита здравља и безбедности на раду представља легитимни интерес послодавца, али он мора бити оствариван у складу са правима и достојанством запослених, при чему обрада оваквих података, којом се задире у здравствену сферу, захтева посебну пажњу, стручност и правну регулисаност.

¹⁸⁰ Правилник о начину и поступку провере алкохолисаности и/или утицаја других опојних средстава запослених у Градској управи града Прокупља од 27.04.2023. године, Прокупље, <https://prokuplje.org.rs/wp-content/uploads/2023/05/pravilnik.pdf>, преузето 15.09.2024. године.

¹⁸¹ *Ibid.*, чл. 3.

¹⁸² Чл. 4. Закона о заштити података о личности.

¹⁸³ *Ibid.*, чл. 17. ст. 1.

¹⁸⁴ *Ibid.*, чл. 17. ст. 2. тач. 8.

8.4.3. Видео-надзор запослених у просторијама послодавца

Систем видео-надзора¹⁸⁵ омогућава руковооцу контролу у реалном времену, затим детекцију кретања, као и интеграцију са другим системима физичко-техничке заштите (Петров, 2021: 23). Данас видео-надзор, захваљујући технолошком развоју пружа широк спектар примене, задирући у приватност и нарушавајући личне податке појединцима. Према Моделу Закона о заштити података о личности видео-надзор обухвата сваки систем којим се може снимати одређени простор, обухватајући и дистрибуцију снимљеног материјала, односно слике или слике и звука, у реалном времену, али без чувања снимљеног материјала.¹⁸⁶ С обзиром на широку употребу видео-надзора и могућности које исти пружа, видео-надзор нашао је примену и у области радних односа. Како и у којој мери употреба видео-надзора утиче на запослене је једно од горућих питања. Највеће сметње у примени видео-надзора запослених јесу психолошки притисак који постоји на стани запослених, нарушавање приватности и достојанства запослених, као и могућност злоупотребе снимљеног материјала (Драгићевић, 2018: 436-437). Насупот томе, позитивне стране видео-надзора по послодавца јесу надгледање и повађавње продуктивности запослених, осигурање безбедности радног окружења и њихове безбедности, као и спречавање недозвољеног и кажњивог понашања, и мера превенције вршења потенцијалних кривичних дела (Žarković, 2015: 174).

У правном систему Републике Србије не постоји закон који на свеобухватан и адекватан начин регулише питање видео-надзора. Уместо тога, на ово питање примењују се одредбе Закона о заштити података о личности. Ипак, сам Закон видео-надзора не регулише експлицитно, што представља нормативни недостатак правног поретка Републике Србије. Овакво стање представља последицу чињенице да ни Општа уредба о заштити података, чије одредбе су импемениране у домаћи закон, не садржи конкретне одредбе којима се ово питање ближе уређује (Diligenski, 2023: 31).

Занимљиво је да ни претходни Закон о заштити података о личности из 2009. године није регулисао питање примене видео-надзора. Повереник је у том смислу начинио и Модел Закона за заштиту података о личности који је указао на недостатак у смеру недефинисања и нерегулисања не само видео-надзора, већ и бројних других

¹⁸⁵ У Закону о приватном обезбеђењу користи се назив видео обезбеђење, док се у теорији користи и назив „телевизија затвореног круга“ и скраћеница CCTV која потиче од термина Close-circuit Television (Rajpoot, Jensen, 2015: 1).

¹⁸⁶ Чл. 3. ст. 1. тач. 14. Модела Закона о заштити података о личности.

проблематичних питања, међутим без обзира на Модел Закона, као и на претходно спроведену јавну расправу, новоусвојеним Законом о заштити података о личности из 2018. године, законодавац је поново изоставио регулисање видео-надзора. Модел је поред одређивања дефиниције видео-надзора детаљно регулисао и обраду података о личности путем видео-надзора, у смислу радног односа. Моделом је прописано да послодавац може, уколико је то неопходно за безбедност лица и имовине, контролу уласка или изласка из пословног простора и ако због природе посла постоји могући ризик за запослене и остале кориснике тог простор, путем видео-надзора да врши обраду података о личности приступа у пословне просторије, док је наредним чланом прописано да се може вршити видео-надзор у пословном простору ако је то неопходно ради заштите безбедности лица или имовине или тајних података и пословних тајни.¹⁸⁷ И у једном и у другом наведеном случају одлука и обавештење о вршењу видео-надзора морају бити донети и упућени у писменој форми од стране послодавца.¹⁸⁸ Модел прописује изричиту забрану вршење видео-надзора у одређеним просторијама, попут гардероба и санитарних просторија¹⁸⁹, а поред просторија прописаних Моделом, просторије у којима није дозвољено увођење видео-надзора су и тоалет, соларијум, ресторан, као и све просторије у којима се драстично задире у приватност особа (Драгићевић, 2018: 438). Моделом Закона послодавци су обавезани да воде Евиденцију о видео-надзору.¹⁹⁰

На проблем нерегулисања видео-надзора је указивао Повереник за информације од јавног значаја и заштиту података о личности у више наврата и у својим публикацијама, које имају посебан значај, поготово за утврђивање праксе у овако нерегулисаним областима.

Из угла Повереника за информације од јавног значаја и заштиту података о личности „...видео-надзор представља обраду података о личности не само у оним ситуацијама када се врши/ сачињава запис о мониторингу физичког лица, односно када долази до систематичног прикупљања таквих записа на одређеном простору, у одређеном временском раздобљу, уз очекивану претпоставку њиховог даљег коришћења, већ и у ситуацијама када такво сачињавање видео-записа изостаје, тј. када видео-надзор представља само „проширено око“ субјекта који врши мониторинг“ (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 89).

¹⁸⁷ *Ibid.*, чл. 38. и чл. 39.

¹⁸⁸ *Ibid.*

¹⁸⁹ *Ibid.*, чл. 39.

¹⁹⁰ *Ibid.*, чл. 36.

Приликом доношења одлуке о постављању видео-надзора потребно је да послодавац одговори на питање са којом сврхом ће се увести видео-надзор и да ли се дати циљ због којег се уводи може постићи и неким другим начином, који би у мањој мери нарушавао приватност запослених (Ковач Орландић, 2018: 136). Начела прописана чланом 5. Закона о заштити података о личности представљају полазне одредбе које морају бити испоштоване приликом постављања система видео-надзора. Начело законитости одређује да мора постојати законит основ обраде података о личности или пристанак запосленог дат у складу са чланом 15. и 16. Закона о заштити података о личности. Начело сврсисходности значи да мора бити тачно одређена сврха за коју се могу користити подаци настали вршењем видео-надзора. Дакле, подаци настали коришћењем видео-надзора у безбедоносне сврхе се не могу користити на терет запосленог како би се конотролисало поштовање радног времена или повреде радне обавезе или дисциплине, за доказвање ових повреда је потребно и коришћење других доказних средстава (Поповић, 2021: 246). У уској вези са начелом ограничења у односу на сврху обраде је начело сразмерности које предвиђа да „подаци који се обрађују морају бити релевантни с обзиром на сврху обраде“ (Драгићевић, 2018: 438). Ако постоји други, мање инвазиван начин обраде података о личности, којим би се постигла иста сврха, онда се не може говорити о сразмерној обради података. Уколико послодавац постави видео-надзор у сврху контроле извршавања радних задатака, реч би била о несразмерној обради и дошло би до непотребног нарушавања приватности (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 94). Систем видео-надзора не сме бити постављен да снима само једног запосленог, а такође постоји и временско ограничење које не дозвољава континуирано надгледање активности запослених (Драгићевић, 2018: 438-439). У прилог томе говори и пресуда Апелационог суда у Новом Саду према којој употреба видео-надзора, који је директно усмерен на радни сто запослене у току читавог радног времена, представља злостављање на раду.¹⁹¹ Стога употреба система видео-надзора на такав начин не представља само пуко кршења прописа о приватности запослених, већ може довести чак и до злостављања на раду. Потребно је да послодавац приликом вршења видео-надзора, сагласно начелу транспарентности, обавести запослене о видео-надзору који се врши. Неопходно је да запослени буду обавештени о примени мере, о циљевима који ће се постићи, као и свим техничким подацима у вези видео-надзора, чувања података и

¹⁹¹ Пресуда Апелационог суда у Новом Саду Гж1 651/13 од 15. маја 2013, [Судске одлуке - Судска пракса - База судске праксе и судских одлука - ВКС \(sud.rs\)](#), преузето 15. 09. 2024. године.

контакт особи која је задужена за руковање подацима који су прикупљени (Драгићевић, 2018, 438). У пракси, послодавци су дужни да приликом вршења видео-надзора поставе визуелна обавештење о упозоравајућем знаку. Сам знак, који се јавља у облику налепнице или табле, садржи графички приказ камере, натпис о посматрању и обавештење о подацима руковаоца података (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 93).

У Публикацији број 3 Повереник таксативно набраја ситуације које се убрајају у изузетне случај у којима се сврха видео-надзора не може постићи мање рестиктивним мерама, и то су обрада у сврху остваривања: 1) безбедности људи, 2) безбедности имовине, 3) заштите тајних података, 4) заштите пословних тајни.

Сходно недостацима и недореченостима у законским регулативама у погледу вршења видео-надзора над запосленима од стране послодавца Повереник има овлашћења да, у случају потребе, у сваком конкретном случају, утврди да ли је с обзиром на природу посла обрада података вршењем видео-надзора оправдана, сразмерна одређеној сврси и правилно конципирана, односно утврђује да ли се циљ обраде може остварити употребом других метода, које су мање инвазивне од видео-надзора (Повереник за информације од јавног значаја и заштиту података о личности, 2018: 107).

8.4.4. Контрола кретања запослених путем ГПС-а

Глобални позициони систем (*Global positions system*) је радионавигациони систем, који се заснива на сателитима и има могућност да одреди тродимензионалну позицију са прецизношћу на нивоу метра и време са тачношћу до 10 наносекунди, на којој год локацији и у које год доба дана.¹⁹² Данас је употреба ГПС система широко распрострањена и примењује се у готово свим сферама – од свемирских истраживања, војних и безбедоносних сврха, преко навигације у саобраћају до система за локацијско праћење и управљање мобилним уређајима и возилима.

Употреба ГПС технологије у погледу система за праћење огледа се у идентификацији, лоцирању и одржавању контакта у реалном времену са једним или више возила (Ноуе, 2016: 35). Посебну пажњу привлачи примена ГПС технологије у области радних односа, где се све чешће користи као средству за праћење кретања и

¹⁹² [GPS - NASA](#), преузето 10.07.2025. године.

активности запослених у радном окружењу, али и ван радних просторија послодавца приликом обављања радних обавеза. Послодавци често поседују возни парк, те ради његовог надзора уводе ГПС систем. Међутим, поставља се питање да ли оваква пракса, омогућавајући послодавцу праћење кретања и локације запосленог у реалном времену, нарушава право на приватност? Затим, уколико долази до нарушавања приватности, намеће се питање у којој мери се нарушава и да ли је нарушавање приватности оправдано или ипак не? Употреба ГПС система у радним односима може довести до прекомерног задирања у приватну сферу запосленог, међутим реч је о мање инвазивној методи надзора од видео-надзора, а разлози који оправдавају увођење се не односе исуључиво на заштиту здравља и безбедности на раду или имовине послодавца, већ се односе на правилну употребу радних средстава и правилно извршење престације рада (Ковач Орландић, 2018: 157). Интереси послодавца могу бити контрола потрошње горива, потрошње средстава на уређајима за плаћање путарине, просечне брзине кретања, пређеног растојања, контрола употребе службених возила у приватне сврхе, затим контрола кретања робе, омогућавање корисницима услуга праћење локације у реалном времену како би били спремни за преузимање робе/извршење услуга и тако даље.

У позитивноправном оквиру Републике Србије, нити Закон о раду нити Закон о заштити података о личности не садрже изричите норме које непосредно регулишу употребу ГПС система за праћење запослених. Уместо тога, примењују се општа правила и начела ових закона, која се односе на заштиту приватности запослених и обраду личних података. Такође, значајну улогу у тумачењу и практичној примени прописа у смислу употребе и коришћења ГПС система у радним односима имају и ставови и пракса Поверника за информације од јавног значаја и заштиту података о личности, који кроз своја мишљења и препоруке настоји да успостави и прецизира јасне границе законитог надзора и заштите права запослених. Поред праксе Повереника, ближи услови употребе ГПС система праћења запослених утврђују се и актима самих послодаваца, најчешће доношењем интерних правилника, којима се уређују правила, сврха, обим и начин примене ових система у радним односима.

Према образложењу Повереника за информације од јавног значаја и заштиту података о личности опрема која је намењена за откривање локације запослених се може инсталирати само ако је неопходно ради постизања легитимне сврхе коју спроводи послодавац, уз услов да њихова употреба не може водити континуираном надзору запослених (Повереник за информације од јавног значаја и заштиту података о

личности, 2025: 45). Дакле, начелно послодавац који има легитимне сврхе може увести ГПС систем за праћење, али је неопходно да такав систем не омогућава послодавцу непрекидан надзор над кретањем запосленог, односно потребно је постојање примарне сврхе која ће остварити уградњом таквог система, а могућност вршења надзора над кретањем запосленог може бити само последица која проистиче из примарне, легитимне сврхе која се постиже.

Повереник такође указује да се приликом коришћења оваквог система морају поштовати и начела предвиђена чл. 5. Закона о заштити података о личности, те посебно начело минимизације и пропорционалности (Повереник за информације од јавног значаја и заштиту података о личности, 2025: 45). Правилником о условима и начину коришћења и одржавања службених возила Градске управе Града Краљева предвиђено је да инсталирани ГПС уређај на возилу може вршити функције праћења и позиционирања возила, брзине и кретања возила, статус активности мотора, пређене километраже, графички приказ пређене руте, могућност праћења путем смарт телефона, креирања различитих извештаја, као и коришћење додатних опција, које се по потреби могу активирати.¹⁹³ У оваквим случајевима, Повереник за информације од јавног значаја и заштиту података о личности могао би, полазећи од конкретних околности и утврђеног обима обраде података, оценити да ли се увођењем наведених функционалности ГПС уређаја прелази граница легитимног и нужног надзора, те да ли долази до задирања у приватност запослених, супротно начелу минимализације и пропорционалности.

Пре инсталације уређаја за мониторинг службених возила послодавац мора утврдити да ли је таква обрада података неопходна и сразмерна сврси која се жели постићи, односно да ли постоје мање инвазивни начини обраде којима се може постићи иста сврха (Повереник за информације од јавног значаја и заштиту података о личности, 2025: 174). Чланом 7. Правилника о надзору над употребом службених возила путем ГПС-а, јавно предузеће „Путеви Србије“ предвиђа да је систем надзора над употребом службених возила посредством ГПС система регулисан тако да буде сразмеран сврси, на начин којим се не угрожава право запослених на приватност, док се истовремено обезбеђује повећена безбедност лица и имовине.¹⁹⁴

¹⁹³ Чл. 5. ст. 2. Правилника о условима и начину коришћења и одржавања службених возила Градске управе Града Краљева, *Сл. лист Града Краљева*, 26/13.

¹⁹⁴ Правилник о надзору над употребом службених возила путем ГПС-а од 05.08.2024. године, Београд, <https://www.putevi-srbije.rs/images/pdf/regulativa/Pravilnik-o-nadzoru-nad-upotrebom-sluzbenih-vozila-putem-GPS.pdf>, преузето 12.07.2025. године.

Послодавац је дужан да на транспарентан начин информише запослене о постављању система за сателитско праћење, применом интерне процедуре, како би запослени благовремено био упознат са чињеницом да се над возилом које користи врши мониторинг (Повереник за информације од јавног значаја и заштиту података о личности, 2025: 45).

Данас, захваљујући технолошким достигнућима, примена ГПС система за праћење се не везује нужно само за постављање уређаја за праћење на службеним возилима, већ је могуће праћење запослених путем специјализованих прслука који у себи садрже локаторе, затим обуће, паметних сатова, таблета и других технолошких иновација. Будуће измене у области заштите приватности и личних података морају регулисати могућност задирања у приватност запослених на начин којим ће се обухватити све промене које са собом доноси развој науке и технологије.

8.5. Институционални механизми заштите права на приватност запослених и санкције у случају његовог кршења

Остваривање и заштита права на приватност запослених не би било могуће без постојања ефикасних институционалних механизма који надгледају примену закона и поступају у случају његовог кршења. У правном поретку Републике Србије, поред судова, кључну улогу у овом контексту има Повереник за информације од јавног значаја и заштиту података о личности, који као самосталан и независан орган надзире примену Закона о заштити података о личности, поступа по притужбама запослених и спроводи надзор над обрадом података о личности.

Заштиту права на приватност пружају судови опште надлежности. Запослени чије је право на приватност повређено имају могућност да се, ради заштите овог права, обрате у грађанскоправном спору месно надлежном вишем суду.¹⁹⁵ У другостепеном поступку, по жалбама, запосленима је на располагању месно надлежан апелациони суд.¹⁹⁶ Запослени могу тужбом покренути поступак ради заштите својих права, која сматрају повређеним поступцима послодаваца у вези са надзором или нарушавањем достојанства или приватности, а ради накнаде материјалне и/или нематеријалне штете, која је настала као последица нарушавања приватности. Међутим, судска пракса је показала да се, у одређеном броју предмета, запослени који се јављају као тужиоци, у

¹⁹⁵ Чл. 25. ст. 1. тач. 7. Закона о уређењу судова, *Сл. Гласник РС*, 10/23.

¹⁹⁶ *Ibid.*, чл. 26. ст. 1. тач. 1.

својим тужбама нису позивали на повреду права на приватност, већ је поступак вођен ради поништаја решења отказа уговора о раду, односно ради утврђења злостављања на раду (Поповић, 2021: 244-245).

Запослени који сматра да су његови подаци обрађивани супротно Закону о заштити података о личности има право да Поверенику за информације од јавног значаја и заштиту података о личности поднесе притужбу.¹⁹⁷ У поступку по поднетој притужби сходно се примењују одредбе Закона о инспекцијском надзору¹⁹⁸ које се односе на представке. Сходно томе, притужбе су иницијаторног карактера за покретање поступка, међутим њихови подносиоци немају својство странке у поступку који се покреће притужбом.¹⁹⁹ Запослени који сматра да одлука Повереника није у складу са законом, има право да поднесе тужбу Управном суду и тако иницира управни спор, у којем може заштити своја права.²⁰⁰ Дакле, одлука Повереника по притужби запосленог је коначна у управном поступку, али запосленом стоји на располагању могућност да покретањем управног спора поништи исту.

Запослени, који сматра да су његови лични подаци обрађивани у супротности одредби Закона о заштити података о личности, чиме је повређено његово право на заштиту личних података, може поднети тужбу којом ће захтевати обавезивање послодавца, као туженог, на давање информације запосленом о обради података о личности и приступу истих, исправку и брисање, ограничавања обраде, преношења, давања и прекида обраде података у складу са законом.²⁰¹

Законодавци су настојали да заштиту личних података обезбеде и инкриминисањем неовлашћеног понашања лица које прикупља податке Кривичним закоником.²⁰² Наиме, кривичним делом „неовлашћено прикупљање личних података“²⁰³ прописана је кривична санкција у виду новчане казне или казне затвора до једне године за неовлашћено прибављање, саопштавање другом или употребу у сврхе за које нису намењени података о личности који се прикупљају, обрађују или користе на основу закона. Кривични законик прописује и квалификовано кривично дело које постоји када кривично дело „неовлашћено прикупљање личних података“²⁰⁴ учини службено лице у

¹⁹⁷ Чл. 82. ст. 1. Закона о заштити података о личности.

¹⁹⁸ Закон о инспекцијском надзору, *Сл. Гласник РС*, 95/18.

¹⁹⁹ *Ibid.*, чл. 18. ст. 3.

²⁰⁰ Чл. 83. ст. 1. Закона о заштити података о личности.

²⁰¹ *Ibid.*, чл. 84. ст. 2. тач. 1-6.

²⁰² Кривични законик, *Сл. Гласник РС*, 94/24.

²⁰³ *Ibid.*, чл. 146. ст. 1.

²⁰⁴ *Ibid.*

вршењу службене дужности, за које је запређена казна затвора до три године.²⁰⁵ Гођење за кривично дело „неовлашћено прикупљање података“ предузима се по приватној тужби, а не по службеној дужности.²⁰⁶ Опређељење законодавца за усвојено законско решење у погледу гођења указује да је законодавац заштиту личних података узео као мање значајну, будући да није предвидео гођење по службеној дужности. Стога, иницирање кривичног поступка за санкционисање оваквог незаконитог понашања је у рукама запослених.

У складу са Европском конвенцијом о заштити људских права и основних слобода запосленима стоји на располагању и могућност покретања поступка пред Европским судом за људска права, чиме се омогућава међународна заштита основних људских права у случају повреде права на приватност.

На крају, значајан сегмент заштите права на приватност у радном односу чини и превенција, односно обавезе послодавца да на јасан и транспарентан начин информисе запослене о свим аспектима обраде њихових података, као и да успостави и примењује јасна правила која ће бити у складу са законом и начелима добре праксе.

IX ЗАКЉУЧАК

Право на приватност запослених представља сложен и правно условљен однос, у коме остваривање права послодавца у погледу обављања делатности, осигурања безбедности и здравља на раду и извршавања законских дужности, зависи од граница које се постављају у погледу приватности запослених. Право на приватност и право на заштиту података о личности запослених чине два међусобно повезана и функционално нераздвојива права, при чему ограничење једног права истовремено одређује и домет другог.

Међународна организација рада настоји да својим посебним правилима систематски уреди питање приватности у радном односу, тако што правила о праву на приватност подређује контексту запослених и кандидата за запослење, чиме превазилази општа правила која приватност штите у апстрактном смислу. Европска унија је, пак, значајно допринела унфикацији и хармонизацији права на приватност запослених, не само у правним системима држава чланица, већ и шире, будући да и државе нечланице своје прописе усклађују са правним тековинама ЕУ, чиме се

²⁰⁵ *Ibid.*, чл. 146. ст. 3.

²⁰⁶ *Ibid.*, чл. 153. ст. 1.

приватност све више стандардизује на наднационалном нивоу. Европски суд за људска права настоји да својим пресудама постави јасне стандарде у области заштите права на приватност, тумачењем члана 8. Европске конвенције о заштити људских права и основних слобода у контексту рада, обезбеђујући доследну и уједначену примену овог права у државама чланицама Савета Европе.

У Републици Србији Закон о раду не пружа довољно разрађен нормативни оквир у овој области, те се у највећој мери примењују општа правила Закона о заштити података о личности. Правилној примени одредаба овог закона у контексту запошљавања знатно доприноси Повереник за информације од јавног значаја и заштиту података о личности, који у својим приручницима, ставовима и мишљењима даје смернице за доследну и закониту примену прописа. Обрада података о личности запослених мора се вршити у складу са основним начелима закона – законитости, сврсисходности, сразмерности и ограниченог чувања података – што подразумева да обрада мора имати законски основ или пристанак запосленог, да се врши само у сврху за коју су подаци прикупљени, у обиму нужном за постизање те сврхе, уз очување интегритета и поверљивости.

Када је реч о основу обраде података, посебна пажња мора се посветити оцени стварне добровољности и правне релевантности пристанка запосленог, јер пристанак дат у односу подређености не представља увек поуздан основ за обраду. Обрада биометријских података, чија је примена све распрострањенија услед технолошког развоја, у начелу је дозвољена, али само ако је строго неопходна и сразмерна сврси која се жели постићи. Мере надзора запослених, као што су контрола употребе службених средстава комуникације, алко-тестирање, тестови на дрогу и видео-надзор, морају бити умерене, пропорционалне и оправдане легитимним циљем. Примена видео-надзора у просторијама као што су гардеробе, санитарни чворови и лифтови, представља недопуштено и прекомерно мешање у приватност запослених.

Повереник за информације од јавног значаја и заштиту података о личности има централну улогу у контроли и унапређењу праксе заштите података. У својим публикацијама и мишљењима он настоји да отклони све недоумице у погледу правилне примене закона, користи своја надзорна овлашћења и указује на уочене недостатке, пропусте и неусклађености у систему заштите података о личности.

Анализа постојећег правног оквира, као и потреба послодаваца да остваре своје интересе и запослених да очувају приватност, показује да је неопходна свеобухватна ревизија и допуна Закона о заштити података о личности. Значајан напредак би

представљало прецизније регулисање области видео-надзора, биометријске обраде података и тестирања запослених, чиме би се успоставио јасан и императиван нормативни оквир, са мање простора за произвољност у пракси. Законодавцу остаје задатак да креира решења која ће одговарати не само тренутним, већ и будућим изазовима које доноси технолошки развој и дигитализација рада.

У том контексту, потребно је развити свеобухватнији концепт „радноправне приватности“, који би објединио класичну заштиту података о личности и шири појам људског достојанства запосленог. У савременом дигиталном окружењу више није довољно штитити запосленог само од неправилне обраде података, већ и обезбедити заштиту његове личности у дигиталном свету - онога што га представља у виртуелном и радном простору, било кроз електронску комуникацију, праћење учинка, примену апликација, система надзора или вештачке интелигенције.

Посебан допринос рада огледа се у указивању на потребу да се право на приватност запослених посматра као динамичка и еволутивна категорија, која се мора прилагођавати технолошким иновацијама, новим облицима рада и надзора. Заштита приватности више не треба да се схвата као ограничење аутономије послодавца, већ као инструмент изградње поверења, безбедности и интегритета радног односа, што у крајњој линији доприноси и већој ефикасности и хуманизацији рада.

Х ЛИТЕРАТУРА

Agencija za zaštitu ličnih podataka i slobodan pristup informacijama od javnog značaja. (2025). Upotreba globalnog pozicionog sistema – GPS u svrhe praćenja službenih vozila: obaveze rukovaoca i prava lica čiji se podaci obrađuju.

Allen, C. (2015). The Four Kinds of Privacy. *Medium*. Преузето 12.08.2025.
<https://medium.com/@christophera/the-four-kinds-of-privacy-bf4b0bf222ac>

Андоновић, С. Прља, Д. (2020). *Основи права заштите података о личности*. Београд: Институт за упоредно право.

Bygrave, L. (2010). The Body as Data? Biobank Regulation via the 'Back door' of Data Protection Law. *Law Innovation and Technology*. vol. 2 (1). 1-25.

Diligenski, A. (2023). Video-nadzor u srpskom pravu; u: Rajić Čalić, J. (ur.). *Uporednopravni izazovi u savremenom pravu – In memoriam dr Stefan Andonović*. Београд: Институт за упоредно право, Правни факултет Универзитета у Крагујевцу. 31-44.

Димитријевић, П. (2011). Правна регулација електронске комуникације и право на приватност. *Зборник радова Правног факултета Универзитета у Источно Сарајеву*. 199–211.

Димитријевић, В. Пауновић, М. Ђерић, М. (1997). *Људска права*. Београд: Београдски центар за људска права.

Драгићевић, М. (2018). Савремене технологије и право запосленог на поштовање приватног живота. *Зборник радова Правног факултета у Нишу*. LVII. 421-441.

Dragičević Prtenjača, M. Zagorec, M. (2023). Ponešto o privatnosti, pravu na privatnost i njezinoj zaštiti u Hrvatskoj kroz kazneno djelo nedozvoljenje uporabe osobnih podataka. *Godišnjak Akademije pravnih znanosti Hrvatske*. Vol. XIV (1). 57-87.

Гајин, С. Ресановић, А. Водинелић, В. В. Миленковић, Д. Цвијан, В. Рељановић, М. (2005). *Заштита података о личности и поверљиви подаци – правни аспекти*. Београд: Фонд за отворено друштво.

Garrett, G. Keleman, D. Schulz, H. (1998). The European Court of Justice, National Governments, and Legal Integration in the European Union. *International Organization*, 52(1). 149-176.

Гасми, Г. Прља, Д. (2020). Право на поштовање приватног живота и право на заштиту података о личности. *Заштита података о личности у Србији*. Београд: Институт за упоредно право. 5-19.

Hendrickx, F. (2022). *Protection of workers' personal data: General principles*. ILO Working Paper 62, Geneva: ILO.

Noque, M. Z. (2016). Basic concept of GPS and its applications. *IOSR Journal of Humanities and Social Science (IOSR-JHSS)*. 21(3). 31-37.

Kovač, N. (2019). Rješavanje u postupcima povrede prava na zaštitu osobnih podataka. *Hrvatska pravna revija*. 5-12.

Ковач Орландић, М. (2018). Право запосленог на приватност и његова заштита (докторска дисертација). Београд: Правни факултет Универзитета у Београду.

Ковачевић, Љ. (2021). *Заснивање радног односа*. Београд: Правни факултет Универзитета у Београду.

Ковачевић, Љ. (2014). Интернет и приватан живот запослених: границе послодавчевих надзорних, дисциплинских и нормативних овлашћења. у: Тодоровић, Д. Петровић, Д. и Прља, Д. (ур.). *Интернет и друштво*. Српско социолошко друштво, Ниш: Универзитет у Нишу – Филозофски факултет, Београд: Институт за упоредно право. 337-352.

Ковачевић, Љ. (2010). Радни однос и право на поштовање приватног живота; у: Шундерић, Б. Лубарда, Б. и Јовановић, П. (ур.). *Остваривање и заштита социјалних права, Зборник радова са Саветовања правника, Златибор, 6-9. октобар 2010*. Београд: Удружење за радно право и социјално осигурање Србије. 166-184.

Krivokapić, D. Krivokapić, Đ. Todorović, I. Komazec S. Petrovski, A. Ercegović, K. (2016). *Vodič za organe vlasti-Zaštita podataka o ličnosti*. Novi Sad: SHARE fondacija.

Cook, P. R. (2002). *Human-Computer Interface Technology: Biometrics – Introduction and Issues*. Princeton, New Jersey: Princeton University.

Лазовић, Д. (2023). *Политика права на приватност и заштита података о личности на интернету: студија случаја: Турске*. Београд: Институт друштвених наука. 219-236.

Letica, I. (2025). BiH ukorak s GDPR-om: Novi Zakon o zaštiti ličnih podataka. *Bloomberg Adria*. Преузето 10.08.2025. <https://ba.bloombergadria.com/komentar/vijesti/78746/novi-zakon-o-zastiti-licnih-podataka-prava-i-obaveze/news>

Maschlanka, L. (2017). European labour law and the protection of workers' privacy – a loophole? (Bachelor Thesis). Enschede: Universiti of Twente, Faculty of Behavioural, Management and Social Sciences (BMS).

Miller, S. Weckert, J. (2000). Privacy, the Workplace and the Internet. *Journal of Business Ethich*. Vol. 28, No. 3. 255-265.

Организација за европску безбедност и сарадњу Мисија ОЕБС-а у Србији. (2019). *Заштита података о личности у сектору безбедности: водич кроз законску регулативу*. Београд.

Пауновић. С. Старчевић, Д. Јеринић, И. (2015). Биометријски идентитет у електронским комуникацијама. *Зборник радова Моћ комуникације 2015*. IV Међународни научни скуп. Београд. 96-106.

Петров, А. (2021). Систем видео надзора у безбедносној заштити лица, имовине и пословања. *16. Конференција са међународним учешћем, Ризик и безбедносни инжењеринг*. Врњачка Бања: Висока техничка школа струковних студија у Новом Саду.

Поповић, М. (2021). Заштита права на приватност на радном месту. *Српска политичка мисао*. 2/2021. 236-250.

Повереник за информације од јавног значаја и заштиту података о личности. (2021). *Заштита података о личности: Ставови и мишљења Повереника*. Публикација бр. 6. Београд.

Повереник за информације од јавног значаја и заштиту података о личности. (2019). *Заштита података о личности у области радних односа Ставови и мишљења Повереника*. Публикација бр. 4. Београд.

Повереник за информације од јавног значаја и заштиту података о личности. (2018). *Заштита података о личности у области радних односа Ставови и мишљења Повереника*. Публикација бр. 3. Београд.

Повереник за информације од јавног значаја и заштиту података о личности. (2012). *Приручник за руковооце*. Београд.

Rajpoot, Q. M. Jensen, C. M. (2015) Video Surveillance: Privacy Issues and Legal Compliance. Denmark: Technical University of Denmark.

Рељановић, М. (2020). Заштита података о личности у радном односу; у: Андоновић, С. Прља, Д. и Дилигенски, А. (ур.). *Заштита података о личности у Србији*. Београд: Институт за упоредно право. 61-92.

Синђелић, Ж. (2012). Право на приватност – кривичноправни, кривичнопроцесни и криминалистички аспекти, докторска дисертација. Београд: Правни факултет Универзитета у Београду.

Станковић, И. (2016). *Јавноправна заштита података о личности*. Ниш: Правни факултет Универзитета у Нишу.

Sućeska, M. Hanić, A. (2014). *Zaštita ličnih podataka u BiH i Srbiji. Sinteza 2014 - Impact of the Internet on Business Activities in Serbia and Worldwide*. 625-629.

Тошић, И. Новаковић, О. (2020.) Утицај нове регулације у области заштите података о личности на рад осигуравајућих друштава. *Зборник радова*. Београд: Институт за упоредно право. 93-104.

Trifunović, V. (2019). *Sudska zaštita prava na privatnost u Bosni i Hercegovini. Bilten sudske prakse. Sud Bosne i Hercegovine*. 9/2019. 66-76.

Vasiljković, J. (2019). *Protection of personal data of employees*. *Pravo – teorija i praksa*. Vol. 36, Br. 10-12. 29-44.

Warren, S. Brandeis, L. (1890). The right to privacy. *Harvard Law Review*. Vol. 4. No. 5.193-220.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

Žarković, I. (2015). Mere elektronskog nadzora zaposlenih i pravo na privatnost na radnom mestu. *Žurnal za kriminalistiku i pravo*. UDC 343.98. 165-182.

XI ОСТАЛА ИСТРАЖИВАЧКА ГРАЂА

Case ECHR of *Antović and Mirković v. Montenegro*, Appl. No. 70838/13 од 28.11.2017. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-178904%22%5D%7D>, преузето 05.09.2025.

Case ECHR of *Bărbulescu v. Romania*, Appl. No. 61496/08, од 05.09.2017. <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-177082%22%5D%7D>, преузето 14.09.2024.

Case ECHR of *Copland v. The United Kingdom*, Appl. No. 62617/00 од 03.04.2007. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22002-2765%22%5D%7D>, преузето 14.09.2024.

Case ECHR of *Fernández Martínez v. Spain*, Appl. No. 56030/07 од 12.06.2014. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-145068%22%5D%7D>, преузето 15.08.2025.

Case ECHR of *Halford v. The United Kingdom*, Appl. No. 20605/92, од 25.06.1997. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-58039%22%5D%7D>, преузето 14.09.2024.

Case ECHR of *Niemitz v. Germany*, Appl. No. 13710/88 од 16.12.1992.
[https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57887%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57887%22]}), преузето 14.09.2024.

Case European Court of Justice of *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v. Minister des Hessischen Kultusministeriums*, C-34/21 од 30.03.2023. [CURIA - Documents](#), преузето 17.08.2025.

Case European Court of Justice of *J.M. v. Pankki S.* C-579/21 од 22.06.2023.
<https://curia.europa.eu/juris/document/document.jsf?jsessionid=854390868FA9C07247E123379BA74EA2?text=&docid=274867&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=21943358>, преузето 17.08.2025.

Европска конвенција о заштити људских права и основних слобода (*Службени гласник Србије и Црне Горе - Међународни уговори*, бр. 9/03).

Кодекс праксе о управљању питањима везаним за алкохол и дроге на радном месту (*Management of alcohol – and drug – related issues in the workplace*. An ILO code of practice, International Labour Office Geneva, 1996).

Кодекс праксе о заштити личних података радника (*Protection of workers' personal data*. An ILO code of practice, International Labour Office, Geneva, 1997).

Кривични законик, *Сл. Гласник РС*, 94/24.

Лисабонски уговор (Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, *Official Journal of the European Communities*, C 306/1).

Међународни пакт о економским, социјалним и културним правима (*Службени лист СФРЈ – Међународни уговори и други споразуми*, бр. 7/71).

Међународни пакт о грађанским и политичким правима (*Службени лист СФРЈ – Међународни уговори и други споразуми*, бр. 7/71).

Мишљење 2/17 о обради података на радном месту (Opinion 2/2017 on data processing at work, Adopted by Article Data Protection Working Party (Brussels, June 2017)).

Мишљење 8/2001 о обради личних података у контексту запослења (Opinion 8/2001 on the processing of personal data in the employment context, Adopted by Article 29 Data Protection Working Party (Brussels, September 2001)).

Модел Закона о заштити података о личности (<https://www.poverenik.rs/sr-yu/%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB-%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%B0-%D0%BE->

[%D0%B7%D0%B0%D1%88%D1%82%D0%B8%D1%82%D0%B8-%D0%BF%D0%BE%D0%B4%D0%B0%D1%82%D0%B0%D0%BA%D0%B0-%D0%BE-%D0%BB%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D0%B8.html](#),

преузето 15.09.2024.

Општа уредба о заштити података о личности (Regulation (EU) 2016/679 of the European Parliament and of the Council, *Official Journal of the European Union*, L119/1, Brussels).

Општи коментар бр. 16 Пакта о грађанским и политичким правима: Члан 17 (Право на приватност) - Право на поштовање приватности, породице, дома и преписке, као и заштиту части и угледа (*CPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* Adopted at the Thirty-second Session of the Human Rights Committee, New York, April 1988).

Полицијска директива (Directive (EU) 2016/680 of the European Parliament and of the Council, *Official Journal of the European Union*, L 119/89, Brussels.)

Повеља Европске уније о основним правима (Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, C 364/1).

Pravilnik o načinu čuvanja i posebnim mjerama tehničke zaštite ličnih podataka, *Sl. glasnik BiH*, 67/09.

Правилник о начину и поступку провере алкохолисаности и/или утицаја других опојних средстава запослених у Градској управи града Прокупља од 27.04.2023. године, Прокупље, <https://prokuplje.org.rs/wp-content/uploads/2023/05/pravilnik.pdf>, преузето 15.09.2024.

Правилник о начину означавања и заштите посебних категорија личних података, *Сл. лист ЦГ*, 011/11.

Правилник о начину претходне провере радњи обраде података о личности, *Службени гласник РС*, број 35/2009.

Правилник о надзору над употребом службених возила путем ГПС-а од 05.08.2024. године, Београд, <https://www.putevi-srbije.rs/images/pdf/regulativa/Pravilnik-o-nadzoru-nad-upotrebom-sluzbenih-vozila-putem-GPS.pdf>, преузето 12.07.2025. године.

Pravilnik o sadržaju i načinu vođenja evidencije o radnicima i zaposlenim kod poslodavaca, *NN* 55/2024.

Правилник о тестирању запослених у Основном суду у Алексинцу на алкохол и друга средства зависности од 19.10.2021. године, Алексинац, [pravilnik o testiranju.pdf \(sud.rs\)](#), преузето 15.09.2024.

Правилник о условима и начину коришћења и одржавања службених возила Градске управе Града Краљева, *Сл. Лист Града Краљева*, 26/13.

Препорука број Р(89)2 о заштити личних података коришћених у сврхе запошљавања (Recommendation No. R (89) 2 of the Committee of Ministers to member States on the processing of personal data used for employment purposes, Adopted by the Committee of Ministers at the 423rd meeting of the Ministers' Deputies (Strasbourg, January 1989)).

Препорука CM/Rec(2015)5 Комитета министара државама чланицама о обради личних података у контексту запошљавања (Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, Adopted by the Committee of Ministers at the 1224th meeting of the Ministers' Deputies (Brussels, April 2015)).

Пресуда Апелационог суда у Новом Саду Гж1 651/13 од 15. маја 2013, [Судске одлуке - Судска пракса - База судске праксе и судских одлука - ВКС \(sud.rs\)](#), преузето 15.09.2024.

Пресуда Управног суда Црне Горе, У. 1792/17 од 26.02.2018. <https://pn2.propisi.net/?di=sp54995&dt=sp&dl=54995>, преузето 18.06.2025.

Пресуда Управног суда Црне Горе, У. 363/23 од 19.09.2023. године, <https://pn2.propisi.net/?di=sp74937&dt=sp&dl=74937>, преузето 18.06.2025.

Пресуда Вишег суда у Подгорици, Гж. 1542/24 од 15.05.2024. године, <https://pn2.propisi.net/?di=sp79577&dt=sp&dl=79577>, преузето 18.06.2025.

Пресуда Вишег суда у Подгорици, Гж. 3730/23 од 23.11.2023. године, <https://pn2.propisi.net/?di=sp75816&dt=sp&dl=75816>, преузето 18.06.2025.

Пресуда Врховног касационог суда Србије Рев2 665/2015 од 23.12.2015. године, <https://www.vrh.sud.rs/sr/%D1%80%D0%B5%D0%B22-6652015-%D0%BF%D0%BE%D0%B2%D1%80%D0%B5%D0%B4%D0%B0-%D1%80%D0%B0%D0%B4%D0%BD%D0%B5-%D0%B4%D0%B8%D1%81%D1%86%D0%B8%D0%BF%D0%BB%D0%B8%D0%BD%D0%B5>, преузето 15.09.2024.

Пресуда Врховног суда Србије Рев2 18/07 од 21.02.2007. године, <https://www.vrh.sud.rs/sr-lat/rev2-1807>, преузето 15.09.2024.

Радни документ о надзору електронских комуникација на радном месту (Working document on the surveillance of electronic communications in the workplace, Adopted by Article 29 Data Protection Working Party (Brussels, May 2002)).

Rešenje Ustavnog suda Republike Hrvatske U-II-565/2025 од 20. маја 2025. године, <https://www.iusinfo.hr/sudska-praksa/USRH2025B565AII?HighlightQuery=565%2f2025>, преузето 21.06.2025. године.

Смернице 07/2020 о појмовима руковаоца и обрађивача података у Општој уредби о заштити података о личности (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Adopted by European Data Protection Board (Brussels, September 2020)).

Смернице за регулисање компјутеризованих база података о личности (Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95, New York, December 1990.).

Универзална декларација о правима човека (Universal Declaration of Human Rights Adopted by General Assembly resolution 217/III, 10.12.1948, Paris).

Упутство за тестирање на дроге и алкохол на радном месту (*Guiding principles on drug and alcohol testing in the workplace as* Adopted by the ILO Interregional Tripartite Experts Meeting on Drug and Alcohol Testing in the Workplace, Oslo, May 1993).

Ustav Bosne i Hercegovine. *Sl. Glasnik BiH*. Br. 25. 2009.

Устав Црне Горе. *Сл. лист ЦГ*. Бр. 01. 2007.

Ustav Republike Hrvatske. *Narodne novine*. Br. 5. 2014.

Устав Републике Србије. *Службени гласник РС*. Бр. 98. 2006.

Закон о електронским комуникацијама. *Службени гласник РС*. Бр. 44. 2010.

Закон о евиденцијама у области рада. *Службени гласник РС*. Бр. 36. 2009.

Закон о инспекцијском надзору. *Службени гласник РС*. Бр. 95. 2018.

Закон о пореској администрацији. *Сл. лист ЦГ*. Бр. 52. 2019.

Zakon o provedbi Opće uredbe o zaštiti podataka Republike Hrvatske. *Narodne novine*, Br. 42. 2018.

Закон о раду. *Службени гласник РС*. Бр. 95. 2018.

Закон о раду Bosne i Hercegovine. *Sl. novine FBiH*. Br. 39. 2024.

Закон о раду Црне Горе. *Сл. лист ЦГ*. Бр. 49. 2008.

Zakon o radu Republike Hrvatske. *Narodne novine*. Br. 64. 2023.

Zakon o radu u institucijama Bosne i Hercegovine. *Sl. glasnik BiH*. Br. 88. 2023.

Закон о слободном приступу информацијама од јавног значаја. *Сл. лист ЦГ*. Бр. 30. 2017.

Zakon o suzbijanju neprijavljenog rada. *Narodne novine*. Br. 151. 2022.

Закон о уређењу судова. *Сл. Гласник РС*. Бр. 10. 2023.

Zakon o zaštiti ličnih podataka. *Sl. glasnik BiH*. Br. 12. 2025.

Zakon o zaštiti ličnih podataka. *Sl. glasnik BiH*. Br. 89. 2011.

Zakon o zaštiti na radu Republike Hrvatske. *Narodne novine*. Br. 96. 2018.

Закон о заштити података о личности. *Сл. лист ЦГ*. Бр. 79. 2008.

Закон о заштити података о личности. *Службени гласник РС*. Бр. 87. 2008.

Закон о здравственој заштити. *Сл. лист ЦГ*. Бр. 8. 2021.

XII САЖЕТАК И КЉУЧНЕ РЕЧИ

Мастер рад се бави остваривањем и заштитом права на приватност запослених у радном окружењу, са посебним освртом на изазове које доноси развој савремених технологија надзора као што су видео-надзор, ГПС праћење и електронска контрола комуникације. Полазиште је да право на приватност, као једно од основних људских права, у савременом добу постаје све угроженије услед технолошког напретка, што захтева стално унапређивање нормативног оквира и механизма заштите.

Основни циљ рада је систематична анализа правне регулативе и праксе у овој области, на међународном, европском и националном нивоу, као и упоредноправни приказ решења у региону. Истраживање има за циљ да укаже на баланс између легитимних интереса послодаваца, као што су безбедност и ефикасност рада, и заштите достојанства, личних података и приватног живота запослених. Рад настоји да идентификује празнине у постојећој регулативи и понуди могуће смернице за њено унапређење.

На међународном плану анализирани су акти Организације уједињених нација и Међународне организације рада, који постављају основна начела заштите приватности радника. У Европи, кључну улогу имају Савет Европе и Европска унија. Савет Европе кроз Европски конвенција о заштити људских права и основних слобода и релевантну судску праксу Европског суда за људска права развија стандарде заштите, док је Европска унија доношењем Опште уредбе о заштити података о личности значајно допринела унификацији правног оквира држава чланица.

Посебна пажња посвећена је упоредноправној анализи, са освртом на законодавство и праксу Црне Горе, Босне и Херцеговине и Хрватске. Анализа је показала да иако постоје сличности у усвајању европских стандарда, одређене разлике и даље постоје, нарочито у домену примене биометријских података, видео-надзора и тестирања запослених.

У домаћем праву, централни пропис представља Закон о заштити података о личности, који је у одређеној мери усклађен са европским правом, али и даље оставља бројне недоумице. Нарочито спорне области обухватају питања обраде биометријских података, законитост видео-надзора, допуштеност алко-тестова и тестова на дрогу, као и надзор службених средстава комуникације. Рад указује на проблем недовољне

јасноће прописа, што у пракси може довести до злоупотреба и повреде права запослених.

Рад обухвата и анализу институционалних механизма заштите, са посебним освртом на улогу Повереника за информације од јавног значаја и заштиту података о личности. Ова институција има кључну улогу у праћењу примене прописа, изрицању мера и подизању свести о значају заштите приватности у радним односима.

У закључку, рад истиче да је потребно јасније дефинисати границе између пословног и приватног живота запослених, те унапредити законодавство како би се обезбедила правна сигурност и спречиле злоупотребе. Посебно је важно развити праксу која ће обезбедити да се мере надзора користе само када су нужно потребне, у мери која је сразмерна легитимној сврси, уз обавезно поштовање достојанства запослених.

Рад даје допринос правној теорији и пракси тиме што пружа свеобухватан приказ изазова у области заштите права на приватност запослених и предлаже могуће смернице за будући развој нормативног оквира.

Кључне речи: приватност, радни однос, запослени, надзор, подаци о личности, заштита података.

XIII ABSTRACT AND KEYWORDS

The Exercise and Protection of Employees' Right to Privacy

The master's thesis deals with the realization and protection of the right to privacy of employees in the workplace, with special emphasis on the challenges brought by the development of modern surveillance technologies such as video surveillance, GPS tracking, and electronic communication monitoring. The starting point is that the right to privacy, as one of the fundamental human rights, in the modern era becomes increasingly endangered due to technological progress, which requires constant improvement of the normative framework and protection mechanisms.

The main aim of the thesis is a systematic analysis of legal regulations and practice in this field, at the international, European, and national levels, as well as a comparative legal review of solutions in the region. The research seeks to point out the balance between the legitimate interests of employers, such as safety and work efficiency, and the protection of the dignity, personal data, and private life of employees. The thesis strives to identify gaps in the existing regulation and to offer possible guidelines for its improvement.

At the international level, the acts of the United Nations and the International Labour Organization, which establish fundamental principles of workers' privacy protection, were analyzed. In Europe, the Council of Europe and the European Union play a key role. The Council of Europe, through the European Convention on Human Rights and the relevant case law of the European Court of Human Rights, develops protection standards, while the European Union, by adopting the General Data Protection Regulation, has significantly contributed to the unification of the legal framework of the member states.

Special attention is dedicated to comparative legal analysis, with reference to the legislation and practice of Montenegro, Bosnia and Herzegovina, and Croatia. The analysis has shown that although there are similarities in the adoption of European standards, certain differences still exist, particularly in the domain of the application of biometric data, video surveillance, and employee testing.

In domestic law, the central regulation is the Law on Personal Data Protection, which is to some extent harmonized with European law, but still leaves numerous ambiguities. Particularly contentious areas include issues of biometric data processing, the legality of video surveillance, the permissibility of alcohol and drug testing, as well as the monitoring of

official means of communication. The thesis points to the problem of insufficient clarity of regulations, which in practice may lead to abuses and violations of employees' rights.

The thesis also includes an analysis of institutional protection mechanisms, with special emphasis on the role of the Commissioner for Information of Public Importance and Personal Data Protection. This institution has a key role in monitoring the implementation of regulations, imposing measures, and raising awareness about the importance of privacy protection in employment relations.

In conclusion, the thesis emphasizes the need to more clearly define the boundaries between the business and private life of employees and to improve legislation in order to ensure legal certainty and prevent abuses. It is particularly important to develop practice that will ensure that surveillance measures are used only when strictly necessary, to the extent proportionate to the legitimate purpose, and with mandatory respect for the dignity of employees.

The thesis contributes to legal theory and practice by providing a comprehensive overview of the challenges in the field of protection of the right to privacy of employees and by proposing possible guidelines for the future development of the normative framework.

Keywords: privacy, employment relationship, employees, monitoring, personal data, data protection.

XIV БИОГРАФИЈА СТУДЕНТА

Марија Миленковић, ауторка рада, рођена је 30. децембра 1999. године у Прокупљу. Детињство је провела у селу Чунгула, где је ниже разреде основног образовања похађала у истуреном одељењу Основне школе „Стојан Новаковић“, а више разреде завршила у матичној школи у општини Блаце. Средње образовање стекла је у Средњој школи у Блацу, где је похађала општи смер гимназије.

Академско образовање започела је у октобру 2018. године уписом основних академских студија на Правном факултету Универзитета у Нишу. Дипломирала је 2023. године и стекла звање дипломирани правник. Стручно усавршавање наставила је исте године уписом мастер академских студија права на Правном факултету Универзитета у Нишу, на смеру Право и информационе технологије, чиме је формално исказала своје интересовање за правне аспекте развоја и примене савремених информационих технологија. Истовремено је показала јаку мотивацију за даље усавршавање и професионални напредак у овој области.

Поред права на приватност, посебно је интересује примена и ефикасност информационих технологија у правним пословима, посебно у контексту правне сигурности и заштите права. Испите на мастер академским студијама положила је у року, са просечном оценом 10,00.

Током основних и мастер академских студија, Марија је учествовала на бројним семинарима, трибинама и стручним предавањима из различитих области права, са циљем усавршавања постојећих и стицања нових знања.

Након стицања звања дипломираног правника, приправнички стаж обавила је у адвокатској канцеларији, где је посебно интересовање исказала за управни поступак и поступак експропријације. Тренутно се припрема за полагање правосудног испита, након чега планира да отвори сопствену адвокатску канцеларију, како би стечена теоријска знања из области информационих технологија применила у пракси.

Говори енглески и руски језик.