Примљено: 05. јун 2023.
Прихваћено: 30. август 2023.

УДК 621.397:342.721(497.11)
COBISS.SR-ID 151621641
DOI: 10.5937/ssb2401057P

# ВИДЕО-НАДЗОР И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ

Златко ПЕТРОВИЋ, помоћник генералног секретара,
Сектор за извештавање и аналитичке послове,
Канцеларија повереника за информације од јавног
значаја и заштиту података о личности,
Република Србија

# ВИДЕО-НАДЗОР И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ

**Сажетак**: *Рад има за циљ да пружи компаративан приказ нормативног уређења видео-надзора на нивоу Европске уније и нормативног уређења видео-надзора у Републици Србији. Сва питања у области заштите података о личности која проистичу из употребе видео-надзора, како у јавном тако и у приватном сектору, нераздвојиво су везана за нормативна решења у Европској унији. Аутор закључује да употреба видео-надзора у Републици Србији није у потпуности и на систематичан начин нормативно уређена, што ствара низ проблема, међу којима се као највећи издваја нарушавање права грађана.*
**Кључне речи**: *видео-надзор, ЕУ, Република Србија.*

## Увод

Видео-надзорни системи представљају ефикасно средство за заштиту лица и имовине, те су као такви веома присутни у свакодневном животу модерног човека. Укупан број ових система је непознаница, управо због лаке набавке и инсталације, те приступачне цене и иновативних решења, која доводе до укрштања функционалности уређаја путем којих се видео-записи могу пратити у реалном времену или накнадно прегледати. Нови облици видео-надзора доносе изузетне могућности праћења, ултрависоке резолуције, те низ нових решења заснованих на вештачкој интелигенцији, попут софтвера за биометријско препознавање у циљу јединствене идентификације лица. Употреба ових система постала је неминовност у читавом савременом свету, било да се користе од стране физичких лица, стамбених зграда, предузетника, компанија или органа власти.

Доступност система видео-надзора многоструко је увећана са развојем интернета, услед масовног присуства дигиталних ИП камера на

тржишту (камере које користе Интернет протокол за пренос података и контролу слике преко рутера и свичера). Једноставна употреба различитих облика видео-надзора омогућила је лако манипулисање снимљеним материјалом, његово издвајање, интервенисање на снимку, те дељење забележеног снимка на платформама попут Youtube или на друштвеним мрежама, што често доводи до нежељених ситуација, које могу имати значајне последице по живот појединца.

Инсталирање и употреба ових система ради различитих врста контроле постали су глобална опсесија, а управо свеопшта присутност видео-надзора и његово стално унапређивање указују на потребу за прецизним и недвосмисленим нормативним уређењем исте области. Неконтролисано и стихијско коришћење ових уређаја нарушава правну сигурност и угрожава приватност физичких лица.

Употреба различитих облика видео-надзора у Републици Србији, како у јавном тако и у приватном сектору, иницира низ питања у области заштите података о личности, која област је у нашој земљи нераздвојиво везана за нормативна решења у Европској унији. Нова европска регулатива у области заштите података о личности има значајан, а може се констатовати и пресудан утицај на регулисање исте области у Републици Србији. Нормативно уређење видео-надзора у Републици Србији, као специфичног облика обраде података о личности, из тог разлога треба сагледати у компаративном смислу, поређењем са прописима у Европској унији.

## I
## Видео-надзор као обрада података о личности, у складу са нормативним актима Европске уније

Два најзначајнија правна акта нове регулативе ЕУ у области заштите података о личности јесу:

– Уредба (ЕУ) 2016/679 Европског парламента и Савета, од 27. априла 2016. године, о заштити физичких лица у односу на обраду података о личности, и о слободном кретању таквих података и о стављању Директиве 95/46/ЕЗ ван снаге (Општа уредба о заштити података), позната као GDPR[1] и
– Директива (ЕУ) 2016/680 Европског парламента и Савета, од 27. априла 2016. године, о заштити појединаца у вези с обрадом

[1] www.poverenik.rs/sr/међународни-документи6/европска-унија.html

података о личности од стране надлежних органа у сврхе спречавања, истраге, откривања или прогона кривичних дела или извршавања кривичних санкција и о слободном кретању таквих података и о стављању ван снаге Оквирне одлуке Савета 2008/977/ПУП, позната као Law Enforcement Directive – LED[2] (код нас се користи израз „Полицијска директива", који није адекватан, јер се овај пропис односи на шири круг субјеката, а не само на полицију. У овом тексту ће израз „Полицијска директива" бити коришћен због опште прихваћености и недостатка адекватнијег израза на српском језику).

Док GDPR регулише општи режим обраде података о личности, „Полицијска директива" регулише посебан режим, који је намењен тзв. „надлежним органима" који врше обраду података о личности у посебне сврхе, односно сврхе спречавања, истраге, откривања или прогона кривичних дела или извршавања кривичних санкција. Обрада података о личности коју врше надлежни органи у друге сврхе (обрачун зараде својим запосленима, кадровска документација и слично) спада у општи режим обраде, који је уређен одредбама GDPR.

Главна разлика између ова два правна акта ЕУ је у начину примене и обавезујућем карактеру, јер директиве захтевају прилагођавање националног законодавства, док се уредбе примењују непосредно у свим државама чланицама ЕУ.

Директива је правни акт ЕУ који поставља циљеве које државе чланице требају постићи, али им оставља одређену флексибилност у избору средстава за постизање тих циљева. Државе чланице морају донети властите националне законе или друге мере како би испуниле захтеве директиве. Директива, у том смислу, није непосредно примењива, што значи да се не примењује непосредно на појединце, привредна друштва и органе власти, већ се мора пренети у национално законодавство.

За разлику од директиве, уредба је правни акт ЕУ који има непосредну примену у свим државама чланицама Европске уније. То значи да се уредба аутоматски примењује и има правну снагу у свим државама чланицама, без потребе за транспоновањем, односно преношењем у национално законодавство. Уредбе се обично користе за уређивање конкретних питања која захтевају једнаку примену и правила у целој ЕУ.

---

[2] www.poverenik.rs/sr/међународни-документи6/европска-унија.html

Оба ова правна акта ЕУ садрже опширне преамбуле, у којима су садржана појашњења појединих института, те на идентичан начин регулишу основне појмове у области заштите података о личности, и то на следећи начин:

- *подаци о личности* су сви подаци који се односе на физичко лице чији је идентитет одређен или се може одредити; физичко лице чији се идентитет може одредити је лице које се може идентификовати посредно или непосредно, посебно помоћу идентификатора као што су име, идентификациони број, подаци о локацији, мрежни идентификатор или помоћу једног или више фактора својствених за физички, физиолошки, генетски, ментални, економски, културни или друштвени идентитет тог физичког лица (члан 3. тачка 1. GDPR и „Полицијске директиве");
- *обрада* је сваки поступак или скуп поступака који се врши над подацима о личности или над скуповима података о личности, аутоматски или неаутоматизовано, као што су прикупљање, евидентирање, организација, структурирање, складиштење, прилагођавање или измена, проналажење, вршење увида, употреба, откривање преносом, ширењем или стављањем на располагање на други начин, усклађивање или комбиновање, ограничавање, брисање или уништавање (члан 3. тачка 2. GDPR и „Полицијске директиве").

Употреба видео-надзорних система који евидентирају присуство и деловање физичких лица у сниманом простору, у том смислу, дефинитивно представља облик обраде података о личности, јер се подаци о личности у форми видео-записа прикупљају, те складиште у претраживе збирке података, које се одређено време чувају и по потреби откривају трећим лицима, након чега се обично аутоматски и бришу. Могућност препознавања физичког лица на забележеном видео-запису управо јесте карактеристика ове специфичне обраде података о личности.

GDPR не регулише експлицитно област видео-надзора, али у члану 35. прописује да је обавезно спровођење процене утицаја на заштиту података о личности у случају обимног систематског праћења јавно доступног простора. Да се под овим праћењем подразумева управо видео-надзор може се утврдити на основу рецитала 91. Преамбуле истог документа („Процена утицаја на заштиту података је у истој мери потребна за обимно праћење јавно доступних подручја, посебно ако се користе оптичко-електронски уређаји ...").

Такође, у члану 88. GDPR прописано је да државе чланице могу законом или колективним уговорима предвидети прецизнија правила са циљем обезбеђивања заштите права и слобода у вези с обрадом података о личности запослених у контексту рада, те да та правила укључују прикладне и посебне мере за заштиту људског достојанства лица на које се подаци односе и његових легитимних интереса и основних права, посебно у вези са транспарентношћу обраде, пренос података о личности унутар групе повезаних друштава или групе предузећа која обављају заједничку привредну делатност, као и система праћења на радном месту.

У рециталу 26. Преамбуле „Полицијске директиве" наведено је: „Свака обрада података о личности мора бити законита, поштена и транспарентна у односу на лица на која се подаци односе и обрађена само у посебне сврхе прописане законом. Ово само по себи не спречава органе за спровођење закона да спроводе активности као што су тајне истраге или видео-надзор. Такве активности се могу обављати у сврху спречавања, истраге, откривања или гоњења кривичних дела или извршења кривичних казни, укључујући заштиту и спречавање угрожавања јавне безбедности, све док су прописане законом и представљају неопходну и пропорционалну меру у демократском друштву, уз дужно поштовање легитимних интереса лица на које се подаци односе."

Смернице Европског одбора за заштиту података (EDPB) представљају драгоцене документе за тумачење прописа у области заштите података о личности, па је потребно напоменути да је исти одбор јануара 2020. године објавио Смернице 3/2019 за обраду података о личности путем видео уређаја (Guidelines 3/2019 on processing of personal data through video devices)[3]. У овим смерницама размотрени су услови законитости обраде путем видео-надзора, откривање видео-снимака трећим лицима, обрада посебних категорија података о личности, права лица на која се подаци односе, обавезе транспрентности и информисања, периоди чувања и обавеза брисања, техничке и организационе мере, те процена утицаја на заштиту података приликом успостављања ових система.

У области посебног режима обраде података о личности, који уређује „Полицијска директива", исти одбор објавио је априла 2023. године Смернице 05/2022 о коришћењу технологије препознавања

[3] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf

лица у области спровођења закона (Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement). У овом документу описује се примена биометријске технологије, спектар њених сврха и примене, поузданост, тачност и ризици за лица на која се подаци односе, а затим се разматра примена исте технологије у односу на Повељу о основним правима ЕУ и Европску конвенцију о људским правима, те „Полицијску директиву", уз практична упутства и примере.

Након усвајања GDPR 2016. године, државе чланице ЕУ су прилагодиле своје националне законе о заштити података о личности овој уредби. Тако је нпр. Република Француска значајно изменила свој Закон о информационим технологијама, подацима и слободама из 1978. године, док је Република Хрватска 2018. године донела Закон о проведби Опће уредбе о заштити података (НН 42/2018). Иако GDPR не регулише експлицитно ову област, овај потоњи закон детаљно уређује видео-надзор, који сврстава у обраду података о личности у посебним случајевима, те исти у чл. 25–29 прописује[4]:

- да се видео-надзор, у смислу одредби овога Закона, односи на прикупљање и даљу обраду података о личности која обухвата стварање снимака који чине или су намењени да чине део збирке података, те ако другим законом није другачије одређено, на обраду података о личности путем система видео-надзора примењују се одредбе овога Закона;
- да се обрада података о личности путем видео-надзора може спроводити само у сврху која је нужна и оправдана за заштиту особа и имовине, ако не претежу интереси лица на која се подаци односе који су у супротности са обрадом података путем видео-надзора, те да видео-надзором могу бити обухваћене просторије, делови просторија, спољна површина објекта, као и унутрашњи простор у средствима јавног превоза, а чији је надзор нужан ради постизања исте сврхе;
- да су руковалац или обрађивач дужни означити да је објекат, односно појединa просторија у њему, те спољна површина објекта под видео-надзором, а ознака треба бити видљива најкасније приликом уласка у периметар снимања, те да обавештење треба да садржи све релевантне информације у складу са одредбама члана 13. GDPR, а посебно једноставну и лако разумљиву слику

[4] Терминологија одредби овог прописа је прилагођена српском језику, за оригинални текст погледати следећи линк: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

уз текст којим се лицима на која се подаци односе пружају следеће информације: – да је простор под видео-надзором; – податке о руковаоцу; – податке за контакт путем којих лице на које се подаци односе може остварити своја права;

– да право приступа подацима о личности прикупљеним путем видео-надзора има одговорна особа руковаоца, односно обрађивача и/или особа коју он овласти, те да ове особе не смеју користити снимке из система видео-надзора супротно утврђеној сврси;
– да систем видео-надзора мора бити заштићен од приступа неовлашћених особа;
– да су руковалац и обрађивач дужни успоставити аутоматизовани систем записа за евидентирање приступа снимцима видео-надзора који ће садржавати време и место приступа, као и ознаку особа које су извршиле приступ подацима прикупљеним путем видео-надзора, те да приступ истим подацима имају надлежни државни органи у оквиру обављања послова из свога законом утврђеног делокруга;
– да се снимци добијени путем видео-надзора могу чувати највише шест месеци, осим ако је другим законом прописан дужи рок чувања или ако су доказ у судском, управном, арбитражном или другом сличном поступку;
– да се обрада података о личности запослених путем система видео-надзора може вршити само ако су уз услове утврђене овим Законом испуњени и услови утврђени прописима којима се регулише заштита на раду и ако су запослени били на примерен начин унапред обавештени о таквој мери, те ако је послодавац информисао запослене пре доношења одлуке о постављању система видео-надзора;
– да видео-надзор радних просторија не сме обухватати просторије за одмор, личну хигијену и пресвлачење;
– да је за успостављање видео-надзора у стамбеним, односно пословно-стамбеним зградама потребна сагласност сувласника који чине најмање 2/3 сувласничких делова, да се истим видео-надзором може обухватити само приступ уласцима и изласцима из стамбених зграда, те заједничке просторије у стамбеним зградама, те да је забрањено коришћење видео-надзора за праћење радног учинка домара, спремачица и других особа које раде у стамбеној згради;

– да је праћење јавних површина путем видео-надзора дозвољено само органима јавне власти, правним лицима с јавним овлашћењима и правним лицима која обављају јавну службу, само ако је прописано законом, ако је нужно за извршење послова и задатака органа јавне власти или ради заштите живота и здравља људи и имовине;
– да наведене одредбе не искључују примену члана 35. GDPR, које прописују обавезу руковаоца за израду процене утицаја на заштиту података о личности (Data protection impact assesement) у случају системског праћења јавно доступног подручја у великој мери.

## II
## Видео-надзор као обрада података о личности, у складу са нормативним актима Републике Србије

Основни разлог доношења новог Закона о заштити података о личности („Сл. гласник РС", број 87/2018) била је међународно прихваћена обавеза Републике Србије из члана 81. ратификованог Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије, са друге стране („Сл. гласник РС – Међународни уговори", број 83/2008), да усклади своје законодавство које се односи на заштиту личних података са комунитарним законодавством и осталим европским и међународним прописима о приватности.

Методологија израде истог закона, садржана у комбиновању превода одредби GDPR и „Полицијске директиве", уз потпуни изостанак одредби преамбула ова два разнородна документа, довела су до законских решења која нису у потпуности дефинисана, нити усклађена са другим прописима Републике Србије, што у пракси доводи до изостанка правне сигурности, како за руковаоце тако и за лица на која се подаци односе. На овом месту важно је напоменути да су експерти Европске комисије, још у мају 2019. године, сачинили Студију[5] у којој

[5] www.poverenik.rs/sr/саопштења/3136-студија-европске-комисије-о-процени-усклађености-закона-о-заштити-података-о-личности-са-прописима-еу-указује-на-потребу-унапређења-овог-закона.html

су упућене бројне критике на текст српског Закона о заштити података о личности, те указано на низ потенцијалних проблема у његовој будућој примени.

Наведена методологија комбиновања општег режима обраде података о личности и посебног режима, који се односи само на обраду коју врше „надлежни органи у посебне сврхе", оставила је низ отворених питања, која могу доћи до изражаја и приликом разматрања видео-надзора, као специфичног облика обраде података о личности. У том смислу, један од изазова јесте и разграничење различитих облика видео-надзора, од којих се поједини користе у сврхе спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности.

Сагласно решењима из GDPR, Закон о заштити података о личности такође прописује да се процена утицаја на заштиту података о личности обавезно врши у случају систематског надзора над јавно доступним површинама у великој мери (члан 54), те да, ако закон који уређује рад и запошљавање или колективни уговор садрже одредбе о заштити података о личности, морају се прописати и посебне мере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини (члан 91).

Члан 2. став 2. Закона о заштити података о личности прописује да одредбе посебних закона којима се уређује обрада података о личности морају бити у складу са овим законом, док члан 100. истог закона прописује да ће се одредбе других закона, које се односе на обраду података о личности, ускладити са одредбама овог закона до краја 2020. године. Међутим, ни после скоро три године од истека овог рока сви ови прописи нису усклађени са истим законом, што се управо види на примеру члана 91. Закона о заштити података о личности.

Наиме, иако Закон о раду („Сл. гласник РС", бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 – одлука УС, 113/2017 и 95/2018 – аутентично тумачење) и други радноправни прописи садрже одредбе о заштити података о личности, посебне мере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно

групе привредних субјеката, као и систем надзора у радној средини до данас нису прописане. У том смислу, системи видео-надзора у радној средини подлежу произвољним тумачењима послодаваца и могу довести до угрожавања достојанства и приватности радника.

У складу са одредбама члана 3. тачка 2. Закона о заштити података о личности, исти закон се не примењује на обраду путем видео-надзора који врши физичко лице за личне потребе, односно потребе свог домаћинства. Међутим, уколико би снимци начињени на овакав начин били дељени са другим лицима, или уколико би, поред приватног простора, био сниман и јавни простор или простор у поседу трећих лица – закон би се примењивао на овакве случајеве.

Законитост обраде података о личности путем видео-надзорних система подразумева постојање правног основа за обраду у складу са чл. 12. и 13. Закона о заштити података о личности. За разлику од обраде коју врше надлежни органи у посебне сврхе, која, као таква, мора бити неопходна за обављање послова надлежних органа и прописана законом, општи режим обраде обухвата шест различитих правних основа, међу којима су за предметну област најрелевантнији легитимни интерес и обављање послова у јавном интересу или извршења законом прописаних овлашћења руковаоца, док пристанак за обраду веома ретко може бити прихватљив основ за обраду.

На овом месту размотрићемо поједине законе Републике Србије који регулишу област видео-надзора.

### *а) Закон о приватном обезбеђењу*

Употреба видео-надзора у Републици Србији детаљније је уређена Законом о приватном обезбеђењу („Сл. гласник РС”, бр. 104/2013, 42/2015 и 87/2018), који уређује обавезно обезбеђење и заштиту одређених објеката, послове и рад правних и физичких лица у области приватног обезбеђења, услове за њихово лиценцирање, начин вршења послова и остваривање надзора над њиховим радом. Поред услуга и послова које врше правна лица и предузетници регистровани за делатност приватног обезбеђења, закон регулише и права и обавезе субјеката који су образовали унутрашњи облик организовања обезбеђења за сопствене потребе, односно самозаштитну делатност.

Исти закон регулише послове техничке заштите, који се врше употребом техничких средстава и уређаја за спречавање противправних радњи према лицима, имовини или пословању, а нарочито за заштиту

од: 1) недозвољеног приступа у просторе и објекте који се обезбеђују; 2) изношења, односно отуђења и неовлашћеног коришћења штићених предмета; 3) уношења оружја, експлозивних, радиоактивних и других опасних предмета и материја; 4) провале, диверзије и насилног напада на објекат или одузимање предмета; 5) неовлашћеног приступа подацима и документацији; 6) заштиту возила за транспорт новца и других превозних средстава; 7) других идентификованих ризика (члан 29).

У смислу овог закона, употребом техничких средстава и уређаја за обезбеђење лица, имовине и пословања сматрају се услуге које се пружају, између осталог, применом уређаја и система за видео-обезбеђење, а иста техничка средства и уређаји могу бити повезани у систем техничке заштите (члан 30). Предметна техничка заштита спроводи се на подручју штићеног објекта или простора, приликом обезбеђења штићених лица, имовине и пословања, или приликом обезбеђења транспорта новца и вредносних пошиљки, а техничка средства која се користе у обављању послова приватног обезбеђења није дозвољено користити на начин којим се нарушава приватност других (члан 31).

Када се послови заштите објекта или простора који се користе за јавну употребу врше уз употребу уређаја за снимање слике, правно лице и предузетник за приватно обезбеђење дужни су да на видљивом месту истакну обавештење да је објекат или простор заштићен видео обезбеђењем, а корисник услуга је обавезан да то прихвати и архивиране снимке чува најмање 30 дана и да их, на захтев, стави на увид овлашћеном полицијском службенику; исти подаци могу се користити само у сврху за коју су прикупљени; забрањено је уступање трећим лицима и јавно објављивање истих података, осим у случајевима предвиђеним законом (члан 32).

Закон о приватном обезбеђењу регулише да се подаци који су прикупљени у вршењу посла приватног обезбеђења могу користити само у сврху за коју су прикупљени и не могу се уступати трећим лицима или јавно објављивати, осим ако је другачије прописано или уговорено, док лице на које се подаци односе има право да захтева да му се прикупљени подаци ставе на увид, што обухвата право на преглед, а о свом трошку и добијање копија података (фотокопију, аудио копију, видео копију, дигиталну копију и сл.) у облику у којем се информација налази, као и да, у складу са прописима, захтева измену или брисање података (члан 68).

У складу са чланом 33. овог закона, Влада Републике Србије донела је Уредбу о минималним техничким условима код обавезне уградње система техничке заштите у банкама и другим финансијским организацијама („Службени гласник РС", број 9/2021), која прописује обавезе банака и других финансијских организација да, у зависности од процењеног нивоа ризика, користе уређаје, опрему и системе техничке заштите који минимално омогућавају:

– изразито велики ниво ризика: праћење кретања у штићеном простору и појединачно штићеним просторијама (контрола приступа и видео обезбеђење) уз видео-запис, који се чува најмање 30 дана;
– велики ниво ризика: праћење кретања у штићеном простору (контрола пролаза и видео обезбеђење) уз видео-запис, који се чува најмање 30 дана;
– умерено велики ниво ризика: праћење кретања око штићеног простора (видео обезбеђење) уз видео-запис, који се чува најмање 30 дана.

На основу овлашћења из истог члана закона, министар унутрашњих послова донео је Правилник о начину вршења послова техничке заштите и коришћења техничких средстава („Сл. гласник РС", бр. 91/2019), који у члану 6. прописује: да уређаји и средства видео обезбеђења који се користе у техничкој заштити морају задовољавати основне захтеве у смислу квалитета, функционалности, минималне резолуције, функционалности у ноћним условима, као и друге захтеве према плану система техничке заштите, а у складу са важећим техничким стандардима; да средства и уређаји видео обезбеђења којима се, поред мониторинга, врши и снимање штићеног објекта или простора морају имати дигитални запис и довољан капацитет меморије за сачињавање записа у трајању од најмање 30 дана, у моду континуалног снимања 24/7 и/или у моду снимања детекцијом кретања, а према плану система техничке заштите, да имају могућност преноса података на преносни медијум у формату читљивом на рачунару, уз потврду одговарајућег воденог жига (watermark) у складу са важећим техничким стандардима, да се спољне камере постављају на такав начин да буду заштићене од уништења, отуђења, климатских услова и да се у видном пољу камере не налазе препреке које би онемогућавале функционалност техничке заштите; да уређаји за снимање у систему видео обезбеђења морају бити смештени у објекту на начин да су заштићени од уништења, отуђења и неовлашћеног приступа (смештај

у одговарајуће ормаре са закључавањем, просторе трезора или других просторија с контролом уласка и приступа или на други начин), да имају могућност аутоматског старта снимања у случају нестанка напајања уређаја, могућност програмирања корисничких шифара и дефинисања права приступа ради контроле и евиденције коришћења уређаја за видео снимање.

Наведене одредбе Закона о приватном обезбеђењу ограничене су на права, обавезе и одговорност правних и физичких лица у области приватног обезбеђења, те субјеката регистрованих за самозаштитну делатност. Међутим, значајно је шири обухват субјеката који користе видео-надзорне системе, с обзиром на њихову лаку доступност. Из наведеног разлога неопходно је на садржајнији начин регулисати ову област, како би и такви облици обраде података о личности били нормирани.

Одредбу да се техничка средства која се користе у обављању послова приватног обезбеђења користе на начин којим се нарушава приватност других неопходно је детаљније регулисати, посебно имајући у виду да кршење исте повлачи прекршајну одговорност.

Обавезу правног лица и предузетника за приватно обезбеђење да на видљивом месту истакну обавештење да је објекат или простор заштићен видео обезбеђењем, те обавезу корисника услуга да то прихвати, неопходно је прецизирати, у контексту транспарентности и пружања информација лицу чији се подаци прикупљају видео-надзорним системом, односно у смислу чл. 21. и 23. Закона о заштити података о личности. У том смислу, лицу које улази у објекат или простор који је заштићен видео обезбеђењем неопходно је пружити основне текстуално-визуелне информације о обради података о личности, те контакт податке (имејл, телефон, QR код, веб страница) путем којих лице може добити тзв „други слој" информација о обради.

Једно од начела обраде за чију примену је одговоран руковалац, у складу са чланом 6. Закона о заштити података о личности, јесте да се подаци о личности морају чувати у облику који омогућава идентификацију лица само у року који је неопходан за остваривање сврхе обраде („ограничење чувања"). Члан 32. Закона о приватном обезбеђењу прописује да је корисник услуга обавезан да архивиране снимке чува најмање 30 дана и да их, на захтев, стави на увид овлашћеном полицијском службенику. Наведена одредба опредељује минимални рок чувања видео-записа, али не и рок након којег се исти снимци морају обрисати, што оставља могућност за произвољна тумачења у примени

исте и отвара простор за непотребно пролонгирање чувања архивираних снимака.

## б) Закон о полицији

Закон о полицији („Сл. гласник РС", бр. 6/2016, 24/2018 и 87/2018) прописује да Министарство унутрашњих послова у сврху организовања послова и стварања услова за рад у Министарству, сагласно делокругу и надлежностима, обавља послове планирања, изградње, коришћења, одржавања и обезбеђивања несметаног функционисања информационих и телекомуникационих система Министарства, укључујући системе видео-надзора и система криптозаштите (члан 11. тачка 8).

Исти закон регулише снимање на јавним местима, као једну од полицијских мера и радњи, и то на следећи начин: Полиција врши надзор и снимање јавног места, ради обављања полицијских послова, коришћењем опреме за видео-акустичке снимке и фотографисање у складу са прописом о евиденцијама и обради података у области унутрашњих послова (став 1); Кад постоји опасност да приликом јавног окупљања дође до угрожавања живота и здравља људи или имовине полицијски службеник овлашћен је да врши снимање или фотографисање јавног скупа (став 2); Ради примене полицијских овлашћења, откривања и расветљавања прекршаја и кривичних дела, као и контроле и анализе обављања полицијских послова, Полиција може вршити аудио и видео снимање поступања полицијских службеника (став 3); Ради постизања циљева из ст. од 1. до 3. овог члана, полицијски службеник може користити превозна и друга средства са или без спољних обележја Полиције, са уређајима за снимање, као и уређаје за снимање и препознавање регистарских таблица (став 4); Намеру да спроведе активности из става 1. овог члана Полиција мора јавно да саопшти, осим када се врши прикривено снимање у складу са Закоником о кривичном поступку (став 5); Подаци прикупљени на начин из ст. од 1. до 4. овог члана чувају се у прописаној евиденцији (став 6); Подаци који се не могу користити у поступку уништавају се у року од годину дана (став 7); Начин снимања на јавном месту и начин саопштавања намере о том снимању прописује министар (став 8).

Правилник о начину снимања на јавном месту и начину саопштавања намере о том снимању („Сл. гласник РС", бр. 111/2020) прописује да се снимањем на јавном месту сматра снимање које полиција врши на јавном месту – простор доступан неодређеном броју лица чији идентитет није унапред одређен, под истим условима или без посебних услова, а визуелни угао који се покрива приликом снимања мора да одговара простору који је неопходан за остваривање законите сврхе снимања, тако да не сме бити већи од неопходног за остваривање те сврхе.

Овај правилник даље прописује: да се снимање на јавном месту врши употребом система за видео-акустичко снимање (видео-надзор) који чине опрема и уређаји за аудио и видео снимање и фотографисање који су постављени на објектима у јавној својини или за ту намену посебно изграђеним објектима; да се снимање на јавном месту врши и употребом друге опреме и уређаја за аудио и видео снимање и фотографисање који су саставни део опреме полицијских службеника, возила, пловила, летелица, као и возила за посебне намене која у свом раду користи Министарство, те да су исти опрема и уређаји: мобилне-акционе камере, камере које се носе на униформи ("body" камере), мобилни телефони, фото апарати, као и други уређаји и средства којима се може забележити аудио и видео снимак или фотографија, осим мерила брзине возила у саобраћају.

У складу са правилником, снимање се врши тако да се евидентирају све битне чињенице и околности у сврху заштите безбедности људи и имовине, праћење јавних скупова, безбедности саобраћаја, граничне контроле, препознавања, односно утврђивања идентитета и проналаска извршилаца кривичних дела, прекршаја и несталих лица, обезбеђивања доказа у вези са извршеним кривичним делима и прекршајима, вршења послова унутрашње контроле, праћења законитости и унапређења рада Министарства, покретања и вођења дисциплинских поступака; када је потребно хитно поступање због опасности од угрожавања живота и здравља људи и имовине или ради спречавања вршења прекршаја и кривичних дела, полицијски службеник врши снимање ако процени да исто може да спроведе на безбедан начин, односно без угрожавања своје и безбедности других лица и уз поштовање људских права и слобода грађана, а тада полицијски службеник усмено саопштава намеру снимања, о чему се обезбеђује доказ – аудио-видео-запис или службена белешка.

Правилник даље прописује да се о намери снимања на јавном месту обавештава јавност путем трајног или привременог знака на месту сталног или привременог снимања, обавештења на званичној интернет страници МУП-а или обавештењем путем медија и других средстава јавног информисања, на начин који омогућава појединцима да се упознају са намером снимања и садрже следеће информације о снимању: слику камере или фото апарата, натпис: „МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА" и званичну интернет адресу МУП-а. У складу са правилником, обавештење о снимању на званичној интернет страници МУП-а садржи додатне информације о руковаоцу и информације о остваривању права лица у вези са снимањем, а, по потреби, додатна обавештења о снимању могу се дати и путем медија и других средстава јавног информисања.

### в) Закон о безбедности саобраћаја на путевима

Закон о безбедности саобраћаја на путевима („Сл. гласник РС", бр. 41/2009, 53/2010, 101/2011, 32/2013 – одлука УС, 55/2014, 96/2015 – др. закон, 9/2016 – одлука УС, 24/2018, 41/2018, 41/2018 – др. закон, 87/2018, 23/2019, 128/2020 – др. закон и 76/2023) прописује снимање саобраћаја и учесника у саобраћају коришћењем одговарајућих средстава, као и документовање прекршаја и других деликата у саобраћају, као једну од посебних мера и овлашћења које се предузимају ради спречавања угрожавања безбедности учесника у саобраћају, односно омогућавања одвијања саобраћаја.

Исти закон у члану 286. прописује: Орган надлежан за послове полиције и орган надлежан за послове саобраћаја имају овлашћење за снимање саобраћаја, у сврху документовања саобраћајних прекршаја, понашања учесника у саобраћају, праћења безбедности и проточности саобраћаја, у оквиру својих надлежности. Евиденција и обрада података прикупљених снимањем саобраћаја уредиће се посебним законом (став 1); Орган надлежан за послове саобраћаја може, уз претходно прибављену сагласност органа надлежног за послове полиције, да овласти управљача пута, јавно предузеће и установу за снимање саобраћаја у сврху из претходног става (став 2); У циљу откривања и доказивања прекршаја полицијски службеници могу користити возила са или без спољних обележја полиције, са уграђеним уређајима за утврђивање прекршаја у саобраћају (возило – пресретач) (став 3);

На возило – пресретач се, док врши утврђивање прекршаја и других деликата и њихово документовање, не односе одредбе овог закона о ограничењу брзине кретања, под условом да тиме не угрожава безбедност саобраћаја (став 4); Возило – пресретач је возило са првенством пролаза када даје прописане посебне светлосне и звучне знаке, најмање једно плаво трепћуће или ротационо светло и звучни знак променљиве фреквенције. Знакови се дају након што прекршај буде откривен и документован у циљу заустављања и даљег процесуирања учиниоца прекршаја, односно другог деликта (став 5); Ближе прописе о начину употребе средстава за снимање и њиховим техничким карактеристикама прописује министар надлежан за послове саобраћаја, уз сагласност Министарства унутрашњих послова (став 6).

Правилник о начину употребе средстава за снимање саобраћаја („Сл. гласник РС", бр. 86/2014) прописује: Средства за снимање саобраћаја подразумевају системе видео-надзора опште намене и системе видео-надзора посебне намене (члан 2); Системи видео-надзора опште намене употребљавају се у сврху праћења безбедности и проточности саобраћаја, понашања учесника у саобраћају и документовања догађаја на путу. Системи видео-надзора посебне намене употребљавају се у сврхе документовања саобраћајних прекршаја и других деликата аутоматским препознавањем регистарских таблица возила којим је прекршај учињен. Системи видео-надзора опште и системи видео-надзора посебне намене могу се употребљавати као појединачни системи и/или као интегрисана целина са међусобно регулисаним начином размене података (члан 3); У сврху снимања саобраћаја користе се фиксни (непокретни) и мобилни, односно системи видео-надзора који се користе у покрету (члан 4); За снимање саобраћаја у системима видео-надзора опште намене користе се фиксне, односно претходно усмерене камере или покретне, односно управљиве камере које омогућавају праћење и снимање ситуација на путу у реалном времену, као и уређаји и средства мобилног надзора (члан 5); За снимање саобраћајних прекршаја у системима видео-надзора посебне намене користе се уређаји и средства мобилног надзора, као и фиксне, односно претходно усмерене камере намењене снимању регистарских таблица и амбијенталних фотографија возила којим је учињен прекршај или неки други деликт (члан 6); За рад средстава за снимање саобраћаја, као дела система видео-надзора, потребно је обезбедити одговарајућу телекомуникациону инфраструктуру и инфраструктуру за напајање електричном енергијом (члан 7); Средства за снимање

саобраћаја, као и сва друга предвиђена опрема и уређаји инсталирају се на предвиђеном камерном месту, односно у или на моторно возило и постављају за рад на начин и у условима прописаним за инсталацију и експлоатацију такве врсте уређаја и опреме. Уређаји и средства фиксног и мобилног надзора за снимање саобраћајних прекршаја у системима видео-надзора посебне намене, као и сва друга предвиђена опрема, инсталирају се на предвиђеном камерном месту, односно у или на моторно возило и/или привремено постављају на одређеним деоницама саобраћајница и користе се на начин и у условима прописаним за техничку експлоатацију такве врсте уређаја и опреме (члан 8); Конкретна позиција и висина камере, као и оријентација објектива дефинишу се посебно, за сваку појединачну локацију, односно моторно возило на начин који ће ускладити позицију и висину у зависности од видног поља камере и захтева корисника, при чему се захтев корисника односи на ситуацију која се посматра (члан 9); Архивирање видео записа са камера, врши се у делу система видео-надзора намењеном за чување података, у претходно дефинисаном формату и облику. Капацитет меморије намењене за архивирање видео-записа мора бити такав да формат видео-записа усклади са захтевом корисника, при чему се захтев корисника односи на конкретан временски интервал за који је предвиђено архивирање видео-записа. Процес архивирања, прикупљања, обраде и коришћења података, до којих се долази преко система фиксног и мобилног надзора за снимање саобраћајних прекршаја у системима видео-надзора посебне намене, регулише се посебно у складу са захтевима корисника (члан 10).

## г) Закон о евиденцијама и обради података у области унутрашњих послова

Закон о евиденцијама и обради података у области унутрашњих послова („Сл. гласник РС”, број 24/2018) уводи термин систем видео-акустичког снимања (видео-надзор), као електронски систем за надгледање и снимање ситуација на неком простору и пренос сигнала с камера на предефинисану локацију. Исти закон уређује ове системе у поглављу које се односи на обраду података системима техничке заштите и комуникационим системима, и то на следећи начин: Министарство, у циљу извршавања послова из свог делокруга, прикупља и обрађује видео и аудио записе коришћењем опреме за видео-аку-

стичко снимање и фотографисање, препознавање и идентификацију лица, аутоматско очитавање исправа и за препознавање регистарских таблица (став 1); Министарство прикупљене податке користи у сврху праћења јавних скупова, повећања безбедности саобраћаја, људи и имовине, граничне контроле, која обухвата вршење провера на граничним прелазима и надзор државне границе ван граничних прелаза, као и у сврху препознавања, идентификације и проналаска извршилаца кривичних дела и несталих лица на основу биометријских података о лицу, обезбеђења доказа за подношење прекршајних и кривичних пријава, вршења послова унутрашње контроле, праћења законитости и унапређења рада Министарства, покретања и вођења дисциплинских поступака (став 2); Министарство може користити средства за снимање слика и бележење аудио и видео-записа других државних органа, органа аутономне покрајине, јединица локалне самоуправе, организација и правних лица, у сврхе из става 2. овог члана (став 3).

Исти закон регулише да МУП обрађује и видео-записе настале у вези са спортским приредбама, те у сврху обављања послова безбедносне заштите одређених лица и објеката и у сврху обављања послова из области саобраћајно-техничких послова безбедности саобраћаја на путевима, у области оспособљавања кандидата за возаче.

У складу са чланом 47. овог закона: МУП води евиденције у којима обрађује податке прикупљене употребом опреме за видео-акустичко снимање и фотографисање, и то: фотографије и аудио и видео-записе лица, возила, догађаја, простора, личне и биометријске податке о лицима, регистарске ознаке возила, датум догађаја, време догађаја, информације о локацији, ЈМБГ, идентификационе бројеве догађаја, податке о власницима возила, податке о возилима и податке о учињеним прекршајима (став 1); Свако изузимање, прегледање, копирање и умножавање видео и аудио записа се евидентира у посебној евиденцији, која садржи: назив организационе јединице која захтева или за чије потребе је извршен увид или направљена копија видео или аудио записа, идентификацију система за видео-акустичко снимање, број захтева, име и презиме полицијског службеника или другог овлашћеног лица које предузима захтеване радње обраде, ЈМБГ, број службене легитимације, податке за иденфикацију видео и аудио записа или фотографија (време и место на којем је аудио и видео-запис или фотографија сачињена, позиција (локација) камере, дужина трајања, назив фајла у ком је запис сачуван, број направљених копија) (став

2); Сви подаци прикупљени коришћењем опреме за видео-акустичко снимање чувају се најкраће 30 дана, односно најдуже пет година, када се прегледом прикупљених података идентификују лица, догађаји и појаве који захтевају предузимање мера и радњи из надлежности Министарства (став 3); Ако су прикупљени подаци потребни за вођење кривичног, прекршајног и дисциплинског поступка чувају се пет година од окончања поступка (став 4).

Поред наведених закона, поједини закони упућују на доношење подзаконских аката у којима фигурира видео-надзор, као облик обраде података о личности.

Тако Закон о основама система образовања и васпитања („Сл. гласник РС", бр. 88/2017, 27/2018 – др. закон, 10/2019, 27/2018 – др. закон, 6/2020, 129/2021 и 92/2023) у члану 108. прописује да Установа доноси акт којим прописује мере, начин и поступак заштите и безбедности деце и ученика за време боравка у установи и свих активности које организује установа, у сарадњи са надлежним органом јединице локалне самоуправе, које је дужна да спроводи, те да Упутство за израду овог акта доноси министар.

У складу са наведеним одредбама, министар просвете донео је Упутство за израду акта којим установе образовања и васпитања прописују мере, начин и поступак заштите и безбедности деце и ученика („Сл. гласник РС", број 67/2022), које у тачки 5. прописује да је, имајући у виду интерес заштите и безбедности деце и ученика у установи и посебно заштите од насиља, изузетно важно да пре измене и допуне постојећих, односно израде нових аката, установа припреми анализу потенцијалних и актуелних ризика у организацији рада установе (просторни, технички, временски и други организациони услови) и то: ... 2) сигурност простора – ограђеност дворишта и степен ризика од могућности приступа трећих лица том простору; осветљеност простора око објекта; видео-надзор; стање приступних рампи и подизних платформи; стање громобрана и инсталација – водоводне, канализационе, електричне и гасне мреже и др.

На основу члана 48. став 2. Закона о заштити лица са менталним сметњама („Службени гласник РС", број 45/13), министар здравља донео је Правилник о ближим условима за примену физичког спутавања и изолације лица са менталним сметњама која се налазе на лечењу у психијатријским установама („Сл. гласник РС", број 94/2013). Исти Правилник у члану 32. прописује: Психијатријска установа у којој постоји систем видео-надзора у просторијама за изолацију дужна је да

обезбеди: 1) да је постојање инсталираног видео-надзора јасно означено; 2) да је посматрање тог лица дозвољено само одређеним здравственим радницима; 3) да не постоји могућност снимања и чувања слика на траци, диску, хард диску или било којем другом формату лица које се налази у изолацији, као и да не постоји могућност слања слика – осим станици за праћење којој приступ има само здравствени радник који је задужен за надзор и лечење тог лица; 4) да престане са коришћењем видео-надзора ако то лице почне да се понаша на начин који нарушава његово достојанство (став 1); Психијатријска установа је дужна да обезбеди да се о постојању инсталираног видео-надзора у просторијама за изолацију упозна лице са менталним сметњама, члан његове уже породице и његов законски заступник (став 2).

Управо наведени подзаконски акт иницира и питање обраде здравствених података, као посебне категорије података о личности, у складу са чланом 17. Закона о заштити података о личности, а посебно имајући у виду да се здравственим подацима сматрају подаци о физичком или менталном здрављу физичког лица, укључујући и оне о пружању здравствених услуга, којима се откривају информације о његовом здравственом стању (члан 4. тачка 16). Иако је обрада посебних врста података о личности начелно забрањена, наведена обрада представља изузетак у складу са законом, посебно имајући у виду да је обрада неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица, те да се врши у контексту пружања здравствене заштите.

Ипак, оба наведена случаја не упућују експлицитно на одредбе Закона о приватном обезбеђењу, као прописа који уређује област видео-надзора, што оставља простор за различита произвољна тумачења, у вези са обавезношћу ангажовања лиценцираних субјеката за област приватног обезбеђења за инсталацију и управљање овим системима техничке заштите. У контексту лаке доступности уређаја за видео-надзор на тржишту, субјекти који имају обавезу употребе видео-надзора, па и они који исту немају, врше набавке и инсталирање ових уређаја без испуњавања адекватних правних, техничких и организационих услова.

Надаље, цитирани Закон о евиденцијама и обради података у области унутрашњих послова прописује да МУП може користити средства за снимање слика и бележење аудио и видео записа других државних органа, органа аутономне покрајине, јединица локалне самоуправе, организација и правних лица. Међутим, поставља се питање

да ли сваки од појединачно наведених субјеката има одговарајући правни основ за успостављање система видео-надзора, да ли опрема коју користе испуњава потребне техничке карактеристике, те да ли предузима одговарајуће организационе, техничке и кадровске мере за спречавање настанка повреде безбедности података о личности. У том смислу, потребно је размотрити на који начин и по којем правном основу ови субјекти уводе систем видео-надзора, како опредељују локације камера, коју технологију снимања користе, колико дуго се забележени снимци чувају, ко има право приступа забележеним снимцима, да ли постоје процедуре за приступање и издвајање забележених снимака итд.

Посебан изазов представљају нова софтверска решења, која омогућавају масовни биометријски видео-надзор. Ова решења заснована су на напретку вештачке интелигенције, који је неслућених размера, а омогућују праћење физичких лица на основу њихових биометријских карактеристика. Употреба ових алата представља изузетно средство за обављање полицијских послова, као што је супротстављање тероризму или проналажење несталих или киднапованих лица, али истовремено носи са собом високе ризике нарушавања приватности грађана, те њиховог константног надгледања. Овакви алати омогућују укрштање биометријских података физичких лица забележених оком камере са већ постојећим масовним збиркама биометријских података грађана, на основу чега се тренутно може идентификовати снимано лице, у реалном времену пратити или накнадно реконструисати његова активност, кретање, локација, друштво итд. Употреба ове технологије оцењена је као веома ризична, а Предлог Уредбе ЕУ о вештачкој интелигенцији[6] предвиђа забрану употребе исте технологије у реалном времену од стране полиције, осим у одређеним изузетним случајевима.

Увођење наведених софтверских решења за потребе полиције у Републици Србији било је најављено још крајем 2018. године, након чега је у надзору, који је спровео Повереник за информације од јавног значаја и заштиту података о личности[7], утврђено да се исти систем још увек не користи, након чега је од стране МУП-а сачињена и процена

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

[7] www.poverenik.rs/sr/архива/саопштења-архива2/3071-повереник-је-спровео-поступак-надзора-у-вези-са-најавом-постављања-видео-камера-од-стране-министарства-унутрашњих-послова.html

утицаја на заштиту података поводом увођења овог система[8], а затим био сачињен и Нацрт закона о унутрашњим пословима, који је прописивао употребу овог система, али који је у два наврата, 2021. и 2022. године, повлачен из јавне расправе. Такође, Повереник је овим поводом 2021. године спроводио поновни поступак надзора у МУП-у[9], где је потврђено да наведена технологија и даље није у употреби.

## Закључак

Употреба видео-надзора у Републици Србији није у потпуности и на систематичан начин нормативно уређена. Овакво стање доприноси правној несигурности, произвољном тумачењу постојећих норми, повредама података о личности и нарушавању приватности грађана. У контексту усклађивања прописа који уређују обраду података о личности са Законом о заштити података о личности, неопходно је извршити компаративну анализу прописа који уређују употребу видео-надзора, ради њихових измена и допуна. Такође, неопходно је посебним прописом генерално регулисати употребу видео-надзора, те јасно прописати услове за његову уградњу и употребу за све субјекте, без остављања простора за различита тумачења. Без свеобухватне, јасне и прецизне нормативе у овој области, грађани не могу ефективно и у пуној мери остварити право на заштиту података о личности, посебно ако нису јасно уређени различити режими видео-надзора, ако они сами немају информације да се видео-надзор уопште врши, те ко је одговоран за њега, коме се могу обратити за копију снимка, те кога могу сматрати одговорним и против кога могу предузимати правне поступке у случају злоупотребе њихових података о личности забележених на видео-запису.

---

8 https://praksa.poverenik.rs/predmet/detalji/FB967E2A-AE57-4B2C-8F11-D2739F-D85A9B

9 www.poverenik.rs/sr/саопштења/3730-повереник-спровео-поступак-надзора-у-муп,-поводом-сумњи-на-употребу-технологије-за-препознавање-лица-facial-recognition-technology.html

# VIDEO SURVEILLANCE AND PERSONAL DATA PROTECTION IN THE REPUBLIC OF SERBIA

Zlatko PETROVIĆ, Assistant Secretary-General,
*Sector for Reporting and Analytical Affairs, Commissioner for Information of Public Importance and Personal Data Protection, Republic of Serbia*

***Summary***

The aim of the paper is to provide a comparative overview of the normative regulation of video surveillance at the level of the European Union and the normative regulation of video surveillance in the Republic of Serbia. All issues in the field of personal data protection arising from the use of video surveillance, both in the public and private sectors, are inextricably linked to normative solutions in the European Union. The author concludes that the use of video surveillance in the Republic of Serbia is not fully and systematically regulated, which creates a number of problems, among which the violation of citizens' rights stands out as the biggest.

**Keywords**: *video surveillance, EU, Republic of Serbia.*