

Република Србија  
МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА  
Секретаријат  
02/4 бр. 072/2-28/19 - 30  
23.09.2019. године  
Београд

РЕПУБЛИКА СРБИЈА  
ПОВЕРЕНИК ЗА ИНФОРМАЦИЈЕ  
ОД ЈАВНОГ ЗНАЧАЈА И ЗАШТИТУ ПОДАТАКА  
О ЛИЧНОСТИ

Број 073-45-1741/19-02  
26-09-2019 20 год  
Београд

ПОВЕРЕНИК ЗА ИНФОРМАЦИЈЕ ОД ЈАВНОГ ЗНАЧАЈА И ЗАШТИТУ ПОДАТАКА  
О ЛИЧНОСТИ

Булевар краља Александра 15, Београд

Предмет: Процена утицаја обраде на заштиту података о личности коришћењем  
система видео надзора.

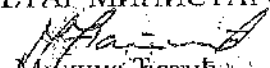
Поштовани,

Обавештавамо Вас да је Министарство унутрашњих послова у складу са чл 54. Закона о  
заштити података о личности извршило процену утицаја на заштиту података о  
личности коришћењем система видео надзора.

С тим у вези, сходно чл. 55. истог закона у прилогу Вам ради давања мишљења  
достављамо извршену процену уз напомену да Вам стојимо на располагању за све  
друге информације од значаја за мишљење.

Прилог: 1 (32 стране формат А4)

СЕКРЕТАР МИНИСТАРСТВА

  
Мироslав Татић

**МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА РЕПУБЛИКЕ СРБИЈЕ**

**ПРОЦЕНА УТИЦАЈА ОБРАДЕ НА ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ  
КОРИШЋЕЊЕМ СИСТЕМА ВИДЕО НАДЗОРА**

**СЕПТЕМБАР 2019**

## САДРЖАЈ

Увод.....	2
1. Законска регулатива којом се уређује систем видео надзора од стране Министарства унутрашњих послова .....	4
1.1. Законом о евиденцијама и обради података у области унутрашњих послова.....	4
Законом о евиденцијама и обради података у области унутрашњих послова .....	4
1.2. Закон о полицији .....	6
2. Надзор Повереника за информације од јавног значаја и заштиту података о личности у вези са постављењем видео-камера од стране Министарства унутрашњих послова .....	8
3. УРЕДБА (ЕУ) 2016/679 ЕУРОПСКОГ ПАРЛАМЕНТА И САВЕТА (GDPR) о заштити појединаца у вези с обрадом података о личности и о слободном протоку таквих података те о стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података).....	10
3.1. Уредба о заштити података (GDPR) .....	10
3.2. Директива (ЕУ) 2016/680 Европског парламента и Савета о заштити појединаца у вези са обрадом података о личности од стране надлежних органа у сврхе спречавања, истраге, откривања или откривања кривичних дела или извршавања кривичних санкција и о слободном преносу таквих података те о стављању ван снаге Оквирне одлуке Савета 2008/977/ПУП.....	11
3.3. Закон о заштити података о личности .....	12
4. Потреба и предности система видео-надзора, утицај људског фактора на употребу система видео-надзора у МУП-у као највећи ризик.....	16
4.1. Потреба за увођењем система видео-надзора.....	16
4.2. Предности коришћења видео-надзора.....	18
4.3. Утицај људског фактора на употребу система видео-надзора.....	19
5. Хронологија увођења интегрисаног система видео-надзора.....	20
5.1. Спровођење пројекта „Сигурно друштво“ од стране МУП-А.....	20
5.2. Опис система видео надзора .....	22
5.3. Администрација системом видео надзора.....	24
Закључак .....	28

У току 2016. године ЕУ је усвојила Општу Уредбу о заштити података о личности, са одредбом да ће се пропис наћи у примени почев од 25.маја 2018.године. Основни циљ Уредбе је хармонизација заштите података о личности на нивоу ЕУ и већи степен контроле за лица чији се подаци обрађују. Циљ прописа је усклађивање регулаторног оквира са актуелним ризицима, узимајући у обзир ризике савременог интернет доба по податке о личности. Уредба се примењује на обраду података о личности, у вези чије дефиниције се уводе и одређене измене управо у смислу осавремењивања. У том контексту, податком о личности се сматрају и *онлине* идентификатори и ИП адресе лица. На исти начин су описани и осетљиви подаци о личности у које спадају расно и етничко порекло, политичка, верска и филозофска уверења, сексуални живот и оријентација, биометријски подаци, синдикално чланство и здравље.

Република Србија је у статусу кандидата за ЕУ и започела је преговоре о приступању ЕУ, и у обавези је да усвоји правне тековине ЕУ. Поглавље 23. приступних преговора се односи на област Правосуђа и основних права. У оквиру овог Поглавља од Републике Србије се захтева усклађивање прописа из области заштите података о личности. С тим у вези у новембру 2018.године Народна скупштина Републике Србије је донела нови Закон о заштити података о личности<sup>1</sup> који је у значајној мери усклађен са принципима Уредбе.

Министарство унутрашњих послова у обављању својих свакодневних послова сагледава могућности за унапређење информационог и телекомуникационог система који би допринео већој заштити животне, личне и имовинске безбедности грађана, спречавања и откривања кривичних дела и проналажање учинилаца, одржавања јавног реда и мира, пружања помоћи у случају опасности, обезбеђење зборов и других окупљања грађана, безбедност, регулисање и контролу саобраћаја на путевима, обезбеђење и контролу преласка државне границе. У том смислу, Министарство унутрашњих послова кроз увођење пројекта „Сигурно друштво“ који подразумева примену најновијих техничких решења за повећање безбедности грађана жели значајно да допринесе расветљавању различитих случаја из домена безбедности учесника у саобраћају, као и из домена опште безбедности.

Системи видео надзора показали су се веома важним у раду полиције и с обзиром на то да се стално усавршавају, те се намеће потреба за увођењем и имплементацијом једног савременог техничког решења, које се користи и у земљама широм Европе, као што су интелигентни системи видео надзора, обједињени под називом „Safe city“.

Имплементација овог решења обухвата проширење броја камерних места новим камерним местима интелигентног видео надзора и постављање система за аутоматску детекцију саобраћајних прекршаја на безбедносно интересантним локацијама на комплетној територији града Београда са свим припадајућим општинама, након чије реализације се очекује битно повећање безбедности свих учесника у саобраћају као и опште безбедности грађана у Београду.

---

<sup>1</sup> „Сл. гласник РС“ бр. 87/2018

## **1. Законска регулатива којом се уређује систем видео надзора од стране Министарства унутрашњих послова**

### **1.1. Законом о евиденцијама и обради података у области унутрашњих послова**

Законом о евиденцијама и обради података у области унутрашњих послова уређује се обрада података о личности у области унутрашњих послова, сврха обраде, права и заштита права лица чији се подаци обрађују, врсте и садржина евиденција у којима се подаци обрађују, рокови чувања, размена података, заштита и контрола заштите података, као и друга питања од значаја за обраду података у области унутрашњих послова.

Обрада података у Министарству унутрашњих послова, врши се у електронској форми у оквиру информационо-комуникационих система, у форми аудио-видео записа и фотографија као и у папирној форми у облику регистара, картотека, дневника и другом облику (евиденције).

Чланом 5. Закона о евиденцијама и обради података у области унутрашњих послова, видео надзор дефинисан је као „систем видео-акустичког снимања“ и представља електронски систем за надгледање и снимање ситуација на неком простору и пренос сигнала с камера на предефинисану локацију;

#### ***Обрада података системима техничке заштите и комуникационим системима***

Истим законом је прописана обрада података системима техничке заштите и комуникационим системима. Члан 13. Закона односи се на *системе за видео-акустичко снимање* и у њему се наводи да Министарство унутрашњих послова, у циљу извршавања послова из свог делокруга прикупља и обрађује видео и аудио записе коришћењем опреме за видео-акустичко снимање и фотографисање, препознавање и идентификацију лица, аутоматско читавање исправа и за препознавање регистарских таблица.

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.

Такође, истим законом предвиђено је да 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.

#### ***Заштита података, мере заштите и евиденције у области видео-акустичних снимања***

Министарство приликом обраде података примењује одговарајуће техничке, кадровске и организационе мере заштите података који се аутоматски обрађују, сагласно усвојеним стандардима и сразмерно ризицима који произлазе из обраде и природе података који се штите, а што је прописано чл. 16. закона. Министарство

предузима одговарајуће безбедносне мере у циљу заштите података од незаконитог уништења или губитка, мењања, неовлашћеног обелодањивања или приступа када се обрада података врши употребом информационо-комуникационих технологија.

Прописане безбедносне мере су:

- 1) онемогућавање неовлашћеним лицима да приступе опреми за обраду података (контрола приступа опреми);
- 2) спречавање неовлашћеног читања, умножавања, измене или уклањања носача података (контрола носача података);
- 3) спречавање неовлашћеног уноса података о личности и неовлашћеног увида, измене или брисања чуваних података о личности (контрола чувања података);
- 4) спречавање неовлашћених лица која користе опрему за пренос података да користе системе за аутоматску обраду података (контрола корисника);
- 5) обезбеђење да лица која су овлашћена да користе систем за аутоматску обраду података имају приступ само подацима о личности који су покривени њиховим овлашћењима за приступ (контрола приступа подацима);
- 6) обезбеђење могућности провере и утврђивања којим органима подаци о личности могу да се доставе или су достављени коришћењем опреме за пренос података (контрола преноса);
- 7) обезбеђење могућности да се провери и утврди који подаци о личности су унети, мењани или брисани у системима за аутоматску обраду података и када и ко је податке о личности унео, мењао или обрисао (контрола уноса);
- 8) спречавање неовлашћеног читања, умножавања, измене или брисања података о личности током преноса података о личности или транспорта носача података (контрола транспорта);
- 9) обезбеђење да, у случају прекида, инсталирани системи могу одмах бити поново успостављени (опоравак);
- 10) обезбеђење да функције система раде без грешке, да се појављивање грешака у функцијама одмах пријави (поузданост) и да чувани подаци о личности не могу да се компромитују грешком у раду система (интегритет).

Примену безбедносних мера у складу са законом којим се уређује област информационе безбедности ближе уређује министар. У Министарству унутрашњих послова у току је израда Правилника о мерама информационе безбедности у информационо-комуникационом систему Министарства унутрашњих послова Републике Србије.

Евидентирање електронске обраде података прописано је чланом 17. Закона. Сваки приступ информационо-комуникационом систему евидентира се у системски журнал. Системски журнал садржи апликациони сигурносни запис у којем се евидентирају све активности, односно трансакције настале употребом одређеног програмског система. Евиденција системског журнала има за циљ заштиту од неовлашћеног коришћења података, као и праћење неовлашћеног покушаја приступа информационо-комуникационом систему.

Спровођење организационих, кадровских и техничких мера заштите података врши посебна организациона јединица Министарства, а што је прописано чл. 18 закона. Организациона јединица представља контакт тачку за континуирану сарадњу са органом надлежним за заштиту података о личности, учествује у поступку или

самостално покреће поступак контроле заштите податка о личности по пријави грађана, органа државне управе, других органа и организација и правних лица, на захтев Сектора унутрашње контроле, овлашћеног лица или комисије надлежне за решавање притужбе грађана у притужбеном поступку и дисциплинског старешине, односно дисциплинске комисије у дисциплинском поступку.

Након спроведеног поступка контроле заштите података о личности, о свим уоченим неправилностима с предлогом мера, надлежна организациона јединица Министарства доставља посебан извештај. Надлежна организациона јединица Министарства министру подноси кварталне извештаје, а органу надлежном за заштиту података о личности доставља годишњи извештај.

Министарство унутрашњих послова ће у наредном периоду определити и „Лице за заштиту података“ у складу са новим Законом о заштити податка о личности.

*Евиденције у области видео-акустичког снимања* прописане су чланом 47. Закона, односно Министарство 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.

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 идентификацију 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).

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. Ако су прикупљени подаци потребни за вођење кривичног, прекршајног и дисциплинског поступка, чувају се пет година од окончања поступка.

## 1.2. Закон о полицији<sup>2</sup>

Чланом 11. Закона о полицији утврђена је надлежност Министарства да обавља послове планирања, изградње, коришћења, одржавања и обезбеђивања несметаног функционисања информационих и телекомуникационих система Министарства, укључујући системе видео надзора и система криптозаштите;

Чланом 52. истог закона утврђен је *правни основ и сврха обраде податка о личности односно предвиђено је да полиција врши надзор и снимање јавног места*, ради обављања полицијских послова, коришћењем опреме за видео-акустичко снимање и

<sup>2</sup>„Сл. гласник РС”, бр. 6/2016, 24/2018 и 87/2018

фотографисање у складу са прописом о евиденцијама и обради података у области унутрашњих послова.

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. 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. 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.

Намеру да спроведе наведене активности, полиција мора јавно да саопшти, осим када се врши прикривено снимање у складу са Закоником о кривичном поступку. Подаци прикупљени на овај начин, чувају се у прописаној евиденцији. Подаци који се не могу користити у поступку, уништавају се у року од годину дана. Начин снимања на јавном месту и начин саопштавања намере о том снимању прописује министар, али акт којим би се ближе уредило снимање на јавном месту и саопштавање намере о том снимању још увек није донет.

Чланом 245. Закона о полицији предвиђено је да полиција и остале организационе јединице Министарства користе средства у јавној својини. Део средстава која Министарство користи чине средства за посебне намене, која су поверљивог карактера.

Непокретности за посебне намене, које користе службе Министарства чија надлежност, организација и поступање има безбедносни или поверљиви карактер, јесу:

- 1) земљиште;
- 2) зграде - службене и друге зграде (пословне просторије, магацини, складишта, гараже и сл.);
- 3) грађевински објекти (монтажни, покретни, привремени и сл.).

Приступ покретним средствима за посебне намене, изван случајева њиховог редовног коришћења, дозвољен је само по претходно прибављеном одобрењу министра.

Покретне ствари за посебне намене, које користе службе Министарства чија надлежност, организација и поступање има безбедносни или поверљиви карактер јесу:

- 1) оружје за службене потребе, у складу са посебним актом, укључујући и муницију и њене елементе, барут, све врсте експлозива, димна и осветљавајућа средства;
- 2) опрема (за експлозивну заштиту; опрема униформисаног састава полиције и специјалних јединица Министарства: одећа, обућа, алпинистичка опрема и ронилачка опрема; идентификационе значке и службене легитимације);
- 3) превозна средства (ваздухопловна превозна средства - хеликоптери и лебделице, као и њихова опрема намењена потребама Министарства; моторна возила - борбена, теренска, теретна, ватрогасна, патролна и друга моторна возила; бродови и чамци - бродови, патролни чамци, диверзантски и извиђачки чамци, бродови и чамци помоћне намене, њихова стандардна и специфична опрема;

4) друга средства (за експлозивну заштиту; средства везе и телекомуникација - радио-опрема, опрема крипто-заштите, скремблери, релејна опрема, анализатори спектра, транспортна мрежа, опрема електронског и видео надзора простора и опреме надзора телекомуникација; средства информационог система - хардвер и софтвер посебне намене и оперативни системи заштите; средства криминалистичке технике - детектори, рендген уређаји, балистичке плоче, посебни материјали криминалистичке технике и друга посебна опрема; системи, уређаји и инструменти за површинско, подводно и ваздушно осматрање и јављање, за оријентацију и навигацију, радари, инфрацрвени уређаји, ласерски мерачи, нишанске справе; основностадо - службени пси, службени коњи и сл.; средства специјалне личне заштитне опреме – заштитна одела, обућа и рукавице, штитови, шлемови, заштитне маске и наочаре, прслуци, антифони и штитници за потребе интервентних, противдиверзионих, ватрогасних јединица и припадника јединица за обезбеђење и заштиту личности).

Под стварима из става 5. овог члана подразумевају се и резервни делови, специјални алати и опрема за одржавање средстава из тог става, друге покретне ствар и за посебне намене које се по својој намени, карактеристикама и својствима, могу уподобити са стварима из става 5. овог члана.

Добра, услуге и радови за потребе и у вези са непокретним и покретним стварима за посебне намене, као и услуге које су у функцији обављања послова из надлежности Министарства и потреба безбедности имају поверљив карактер у смислу става 2. овог члана.

Начин набавке средстава за посебне намене без јавног оглашавања прописује Влада.

## **2. Надзор Повереника за информације од јавног значаја и заштиту података о личности у вези са постављењем видео-камера од стране Министарства унутрашњих послова**

Капиталним пројектом „Видео надзор у саобраћају- Фаза1“ у току 2017. год. Министарство унутрашњих послова реализовало је реконструкцију постојећег видео надзора града Београда, као и реконструкцију Командно-оперативног центра Полицијске управе за град Београд, где је смештен „data center“ система и главни кориснички центар Дежурне службе ПУ за град Београд.

Капиталним пројектом „Видео надзор у саобраћају – Фаза 2“, наставља се реализација пројекта „Безбедан град“ на целокупној територији града Београда. Предвиђено је да се на више од 800 нових локација (камерних места) поставе камере, при чему ће се реализација пројекта вршити у фазама, у укупном трајању од три године.

Повереник за информације од јавног значаја је покренуо поступак надзора над спровођењем и извршавањем Закона о заштити података о личности у вези са постављењем видео-камера од стране Министарства унутрашњих послова, са становишта обраде података о личности.<sup>3</sup>

<sup>3</sup> <https://www.poverenik.rs/sr/>, Саопштење.

У складу са Законом о заштити података о личности, у надлежности Повереника је да у случају ако је вероватно да ће нека врста обраде, посебно употребом нових технологија и узимајући у обзир природу, обим, околности и сврху обраде, проузроковати висок ризик за права и слободе физичких лица даје мишљење пре започињања радње обраде.

Такође, Закон о заштити података о личности, прописује обавезу Министарства унутрашњих послова (МУП), као руковођа података, да, у вези са најављеним системом видео-надзора, спроведе процену утицаја на заштиту података о личности, те да о истом прибави и претходно мишљење Повереника.

Повереник је у спроведеном поступку надзора затражио изјашњење о планираној обради података, правном основу, сврси, техничким карактеристикама и свим другим релевантним чињеницама, те је од стране Министарства унутрашњих послова обавештен о следећем:

- да полиција има овлашћење да 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, у складу са чланом 52. Закона о полицији;
- да МУП, има овлашћење да у циљу извршавања послова из свог делокруга прикупља и обрађује видео и аудио записе коришћењем опреме за видео-акустичко снимање и фотографисање, препознавање и идентификацију лица, аутоматско читавање исправа и за препознавање регистарских таблица, те 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, у складу са чланом 13. Закона о евиденцијама и обради података у области унутрашњих послова;
- да је предметни систем видео-надзора још у фази тестирања, те да се у овој фази не користе реални, већ само тестни подаци и
- да систем видео надзора неће бити повезан за збиркама биометријских података грађана чија је сврха обраде уређена посебним законима.

Министарство унутрашњих послова је Поверенику за информације од јавног значаја и заштиту података о личности доставило све релевантне информације о техничким карактеристикама система видео надзора чије увођење се планира, као и предвиђене мере безбедности података. Након увида у достављене информације од стране Повереника, овом Министарству је указано на неопходност израде процене утицаја употребе овог система на заштиту података о личности, као обавезу руковођа података у складу са новим Законом о заштити података о личности.

Повереник константно прати активности МУП-а на успостављању овог система, као и његово даље функционисање са становишта заштите података о личности, те у том смислу поступак надзора још увек није окончан.

### 3. УРЕДБА (ЕУ) 2016/679 ЕУРОПСКОГ ПАРЛАМЕНТА И САВЕТА (GDPR) о заштити појединача у вези с обрадом података о личности и о слободном протоку таквих података те о стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података)

#### 3.1. Уредба о заштити података (GDPR)

Право на заштиту података о личности је право које се суштински тиче сваког људског бића, а новина на међународном плану у области заштите података јесте да је 2018. године почела примена Уредбе о заштити података (ГДПР).

Према члану 2. Уредбе овај пропис се примењује на обраду података о личности која се у целости или делимично обавља аутоматски и на неаутоматизовану обраду података о личности који чине део збирке података или су намењени збирци података. Бројне су новине прописане Уредбом у односу на Директиву 95/46/ЕЗ. Обрада података из периода деведестих, много пре друштвених мрежа и масовне употребе паметних технологија и уобичајеног аутоматизованог начина обраде података, доживела је знатне промене.

У погледу новина за појединце, важно је истаћи да је један од основних циљева Уредбе, оснаживање појединца чији се подаци обрађују. С тим у вези је и обављање Процене утицаја на заштиту података („Personal Data Impact Assessment“) (члан 35.). Процена утицаја на заштиту података постаје обавезни предуслов за отпочињање обраде података о личности која би могла да представља већи ризик за приватност. Спровођење процене увек је неопходно у случају систематске и обимне обраде у циљу процене личних аспеката неког лица која се заснива на аутоматизованој обради, укључујући и израду профила, и која је основ за доношење одлука које производе правно дејство у односу на физичко лице или на сличан начин значајно утичу на физичко лице. Ова процена је такође неопходна у случају масовне обраде посебних категорија података о личности или података који се односе на кривичну и прекршајну осуђиваност; или обимног систематског надзора јавно доступног простора. Ако би се проценом утицаја на заштиту података показало да би, у случају да руковалац не обезбеди мере за ублажавање ризика, обрада довела до високог ризика, тада је руковалац дужан да контактира надзорно тело и да му достави, између осталог, информације о сврси и средствима обраде, заштитним мерама, спроведеној процени утицаја итд.

Службеник за заштиту података (члан 37.) – Уредба уводи обавезу именовања службеника за заштиту података увек када обраду врши орган јавне власти, осим судова који поступају у оквиру своје судске надлежности, када се основне делатности руковаоца или обрађивача састоје из радњи обраде које због своје природе, обима и/или сврхе захтевају редовно и систематско масовно праћење лица на која се подаци односе, или се основне делатности руковаоца или обрађивача састоје из масовне обраде

посебних категорија података и података о личности који се односе на кривичну и прекршајну осуђиваност.

Заштита података о личности за Републику Србију је питање које се усклађује у процесу приступања Европској унији и у оквиру Поглавља 23 (Правосуђе и основна права), као и Поглавља 24 (Правда, слобода и безбедност). Основни разлог за доношење Закона је усклађивање са регулативом Европске уније, односно гарантовање истог степена заштите података о личности као у државама чланицама Европске уније. Увођење новог законског решења део је обавеза Републике Србије у процесу придруживања Европској унији. Закон се у великој мери ослања на решења која су предвиђена Уредбом о заштити података о личности (ГДПР).

3.2. Директива (ЕУ) 2016/680 Европског парламента и Савета о заштити појединаца у вези са обрадом података о личности од стране надлежних органа у сврхе спречавања, истраге, или откривања кривичних дела или извршавања кривичних санкција и о слободном преносу таквих података те о стављању ван снаге Оквирне одлуке Савета 2008/977/ПУИ

Према Директиви свака обрада података мора бити законита, поштена и транспарентна у односу на појединце на које се односи те обављена само у посебне сврхе утврђене законом. То само по себи не спречава надлежне органе за извршавање законодавства у обављању активности као што су тајне истраге или видео надзор. Такве активности могу се спровести у сврхе спречавања, истраге, откривања или прогона кривичних дела или извршавања кривичних санкција, укључујући заштиту од претњи јавној безбедности и њихово спречавање, под условом да су утврђене законом и представљају нужну и сразмерну меру у демократском друштву уз дужно поштовање легитимних интереса појединца на које се подаци односе. Начело заштите података у погледу поштене обраде одвојено је од појма права на поштено суђење, како је утврђено у члану 47. Повеље и у чл. 6. Европске конвенције за заштиту људских права и основних слобода. Појединце би требало упознати с ризицима, правилима, заштитним мерама и правима у вези с обрадом њихових података о личности и начином остваривања њихових права у вези с обрадом. Посебне сврхе обраде података о личности би требале бити јасно одређене и легитимне те утврђене у тренутку прикупљања података. Подаци о личности би требали бити сразмерни и битни за потребе за које се обрађују. Нарочито би требало обезбедити да се не прикупљају сувишни подаци и да се не чувају дуже него што је нужно за потребе за које се обрађују. Подаци о личности могли би се обрађивати само ако се сврха обраде оправдано не може постићи другим средствима. Ради обезбеђивања да се подаци не чувају дуже но што је потребно, руковалац података требао би одредити временске рокове за брисање или периодично преиспитивање.

Овом Директивом утврђују се посебна правила у вези са заштитом појединаца у погледу обраде података о личности од стране надлежних органа у сврхе спречавања, истраге, откривања кривичних дела или извршавања кривичних санкција, укључујући заштиту од претњи јавној безбедности и њихово спречавање.

Јавност у Републици Србији није на адекватан начин упозната са одредбама Директиве и тежњом надлежних органа да своје поступање ускладе са прописима ЕУ. У начелу је сва пажња јавности усмерена ка одредбама Уредбе о заштити података али

се одредбе Директиве којом се посебно уређује обрада података о личности од стране државних органа надлежних за спречавање, истраге, откривање кривичних дела или извршавање кривичних санкција, укључујући и заштиту од претњи јавној и националној безбедности у јавности уопште не спомиње.

Нови Закон о заштити података о личности је по угледу на поменути Директиву јасно извојио поједине радње обраде и утврдио посебан режим обраде података од стране надлежних органа међу којима је свакако и Министарство унутршњих послова.

### 3.3. Закон о заштити података о личности

Закон о заштити података о личности<sup>4</sup> у Републици Србији, чија је примена почела 22.08.2019. година, прописује пуно новина у овој области. По узору на Уредбу и Директиву овај закон садржи одредбе о новим правима лица чији се подаци обрађују, а тиме и о новим обавезама руковалаца и обрађивача података, и мења улогу Повереника увођењем бројних нових обавеза.

Предмет овог закона је уређење права на заштиту физичких лица у вези са обрадом података о личности и слободни проток таквих података, начела обраде, права лица на које се подаци односе, обавезе руковалаца и обрађивача података о личности, кодекс поступања, пренос података о личности у друге државе и међународне организације, надзор над спровођењем овог закона, правна средства, одговорност и казне у случају повреде права физичких лица у вези са обрадом података о личности, као и посебни случајеви обраде.

*Овим законом уређује се и право на заштиту физичких лица у вези са обрадом података о личности коју врше надлежни органи 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, као и слободни проток таквих података.*

Чланом 3. Закона прописана су значења израза:

„*обрада података о личности*” је свака радња или скуп радњи које се врше аутоматизовано или неаутоматизовано са 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 чинињење доступним, упоређивање, ограничавање, брисање или уништавање (у даљем тексту: обрада);

„*збирка података*” је сваки структурисани скуп података о личности који је доступан у складу са посебним критеријумима, без обзира да ли је збирка централизована, децентрализована или разврстана по функционалним или географским основама;

„*руковалац*” је физичко или правно лице, односно орган власти који самостално или заједно са другима одређује сврху и начин обраде. Законом којим се одређује сврха и начин обраде, може се одредити и руковалац или прописати услови за његово одређивање;

<sup>4</sup> „Сл. гласник РС”, бр.87 од 13. новембра 2018.

„обрађивач“ је физичко или правно лице, односно орган власти који обрађује податке о личности у име руковођаца;

„прималац“ је физичко или правно лице, односно орган власти коме су подаци о личности откривени, без обзира да ли се ради о трећој страни или не, осим ако се ради о органима власти који у складу са законом примају податке о личности у оквиру истраживања одређеног случаја и обрађују ове податке у складу са правилима о заштити података о личности која се односе на сврху обраде;

„надлежни органи“ су:

а) органи власти који су надлежни за спречавање, истрагу и откривање кривичних дела, као и гоњење учинилаца кривичних дела или извршење кривичних санкција, укључујући и заштиту и спречавање претњи јавној и националној безбедности;

б) правно лице које је за вршење послова из подтачке а) ове тачке овлашћено законом

Законитост обраде је прописана чланом 12. - Обрада је законита само ако је испуњен један од следећих услова:

1) лице на које се подаци о личности односе је пристало на обраду својих података о личности за једну или више посебно одређених сврха;

2) обрада је неопходна за извршење уговора закљученог са лицем на које се подаци односе или за предузимање радњи, на захтев лица на које се подаци односе, пре закључења уговора;

3) обрада је неопходна у циљу поштовања правних обавеза руковођаца;

4) обрада је неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица;

5) обрада је неопходна у циљу обављања послова у јавном интересу или извршења законом прописаних овлашћења руковођаца;

6) обрада је неопходна у циљу остваривања легитимних интереса руковођаца или треће стране, осим ако су над тим интересима претежнији интереси или основна права и слободе лица на које се подаци односе који захтевају заштиту података о личности, а посебно ако је лице на које се подаци односе малолетно лице.

*Обавезе руковођаца прописане су чл.41.* - Руковалац је дужан да предузме одговарајуће техничке, организационе и кадровске мере како би обезбедио да се обрада врши у складу са овим законом и био у могућности да то предочи, узимајући у обзир природу, обим, околности и сврху обраде, као и вероватноћу наступања ризика и ниво ризика за права и слободе физичких лица.

*Мере заштите (чл.42.)* - Узимајући у обзир ниво технолошких достигнућа и трошкове њихове примене, природу, обим, околности и сврху обраде, као и вероватноћу наступања ризика и ниво ризика за права и слободе физичких лица који произилазе из обраде, руковалац је приликом одређивања начина обраде, као и у току обраде, дужан да:

1) примени одговарајуће техничке, организационе и кадровске мере, као што је псеудонимизација, које имају за циљ обезбеђивање делотворне примене начела заштите података о личности, као што је смањење броја података;

2) обезбеди примену неопходних механизма заштите у току обраде, како би се испунили услови за обраду прописани овим законом и заштитила права и слободе лица на која се подаци односе.

Руководалац је дужан да сталном применом одговарајућих техничких, организационих и кадровских мера обезбеди да се увек обрађују само они подаци о личности који су неопходни за остваривање сваке појединачне сврхе обраде. Та се обавеза примењује у односу на број прикупљених података, обим њихове обраде, рок њиховог похрањивања и њихову доступност.

**Обрађивач (чл.45.)** - Ако се обрада врши у име руководаца, руководалац може да одреди као обрађивача само оно лице или орган власти који у потпуности гарантује примену одговарајућих техничких, организационих и кадровских мера, на начин који обезбеђује да се обрада врши у складу са одредбама овог закона и да се обезбеђује заштита права лица на које се подаци односе.

**Евиденција радњи обраде (чл.47.)** - Руководалац и његов представник, ако је одређен, дужан је да води евиденцију о радњама обраде за које је одговоран.

**Безбедност обраде (чл.50.)** - У складу са нивоом технолошких достигнућа и трошковима њихове примене, природом, обимом, околностима и сврхом обраде, као и вероватноћом наступања ризика и нивоом ризика за права и слободе физичких лица, руководалац и обрађивач спроводе одговарајуће техничке, организационе и кадровске мере како би достигли одговарајући ниво безбедности у односу на ризик.

Законом се уводи обавеза анализе ризика пре започињања радњи обраде, а ако је ризик високог нивоа прописује се неопходност тражења мишљења надзорног органа, односно Повереника

**Процена утицаја на заштиту података о личности (чл.54.)** - Ако је вероватно да ће нека врста обраде, посебно употребом нових технологија и узимајући у обзир природу, обим, околности и сврху обраде, проузроковати висок ризик за права и слободе физичких лица, руководалац је дужан да пре него што започне са обрадом изврши процену утицаја предвиђених радњи обраде на заштиту података о личности.

Ако више сличних радњи обраде могу проузроковати сличне високе ризике за заштиту података о личности, може се извршити заједничка процена. Приликом процене утицаја руководалац је дужан да затражи мишљење лица за заштиту података о личности.

Процена утицаја обавезно се врши у случају:

1) систематске и свеобухватне процене стања и особина физичког лица која се врши помоћу аутоматизоване обраде података о личности, укључујући и профилисање, на основу које се доносе одлуке од значаја за правни положај појединца или на сличан начин значајно утичу на њега;

2) обраде посебних врста података о личности или података о личности у вези са кривичним пресудама и кажњивим делима, у великом обиму;

3) систематског надзора над јавно доступним површинама у великој мери.

Повереник је дужан да сачини и јавно објави на својој интернет страници листу врста радњи обраде за које се мора извршити процена утицаја, а може да сачини и објави и листу врста радњи обраде за које процена није потребна.

Процена утицаја најмање мора да садржи:

1) свеобухватан опис предвиђених радњи обраде и сврху обраде, укључујући и опис легитимног интереса руковоаца, ако он постоји;

2) процену неопходности и сразмерности вршења радњи обраде у односу на сврхе обраде;

3) процену ризика за права и слободе лица на које се подаци односе ;

4) опис мера које се намеравају предузети у односу на постојање ризика, укључујући механизме заштите, као и техничке, организационе и кадровске мере у циљу заштите податка о личности и обезбеђивања доказа о поштовању одредби овог закона, узимајући у обзир права и легитимне интересе лица на које се подаци односе и других лица.

*Процена утицаја обраде коју врше надлежни органи у посебне сврхе најмање мора да садржи свеобухватан опис предвиђених радњи обраде, процену ризика по права и слободе лица на које се подаци односе, опис мера које се намеравају предузети у односу на постојање ризика, укључујући механизме заштите, као и техничке, организационе и кадровске мере у циљу заштите податка о личности и обезбеђивања доказа о поштовању одредби овог закона, узимајући у обзир права и легитимне интересе лица на које се подаци односе и других лица.*

**Претходно мишљење Повереника (чл.55.)** - Ако процена утицаја на заштиту података о личности, која је извршена у складу са чланом 54. овог закона, указује да ће намераване радње обраде произвести висок ризик ако се не предузму мере за умањење ризика, руковалац је дужан да затражи мишљење Повереника пре започињања радње обраде.

Ако обраду врши надлежни орган у посебне сврхе, руковалац, односно обрађивач је дужан да затражи мишљење Повереника пре започињања радњи обраде које ће довести до стварања нове збирке података у случају да:

1) процена утицаја на заштиту података о личности, која је извршена, указује да ће намераване радње обраде произвести висок ризик ако се не предузму мере за умањење ризика;

2) врста обраде, а посебно ако се користе нове технологије, механизми заштите или поступци, представљају висок ризик за права и слободе лица на које се подаци односе.

Уз захтев за мишљење, руковалац је дужан да Поверенику достави податке о:

1) дужностима руковоаца, и ако постоје, заједничких руковоаца и обрађивача који учествују у обради, посебно ако се ради о обради која се врши унутар групе привредних субјеката;

2) сврхама и начинима намераване обраде;

3) техничким, организационим и кадровским мерама, као и механизмима заштите права и слобода лица на које се подаци односе у складу са овим законом;

4) контакт подацима лица за заштиту података, ако је оно одређено;

5) процени утицаја на заштиту података о личности ;

6) свим другим информацијама које затражи Повереник.

Ако обраду врши надлежни орган у посебне сврхе, руковалац је дужан да Поверенику достави податке о процени утицаја на заштиту података о личности, а на захтев Повереника и друге информације које су од значаја за његово мишљење о радњама обраде, а посебно ризику по заштиту података о личности лица на које се подаци односе и механизмима заштите његових права.

Чланом 56. прописано је да руковалац и обрађивач одређују лице за заштиту података о личности.

Закон такође уводи и бројне друге новине, као што су обавезујућа пословна правила, сертификација, одређивање лица за заштиту података о личности, као и кодекс поступања и потпуно уређење обраде података о личности коју врше надлежни органи у сврхе спречавања, истраге, откривања или гоњења кривичних дела или извршења кривичних санкција, те елементе уговора или другог обавезујућег акта на основу кога се врши поверавање обраде података обрађивачу.

#### 4. Потреба и предности система видео-надзора, утицај људског фактора на употребу система видео-надзора у МУП-у као највећи ризик

##### 4.1. Потреба за увођењем система видео-надзора

Потреба за увођење квалитетног система видео-надзора од стране Министарства унутрашњих послова јавила услед чињенице да се у савременом свету све безбедносне службе сусрећу са све већим бројем изазова у свом раду. С тим у вези неопходно је применити технике које имају за циљ отежавање вршења криминалних радњи, као и представљање криминала опаснијим, мање пожељним, мање оправданим и мање провокативним. Видео-надзор се може сврстати у мере формалног надзора, којима се делује на перцепцију ризика код потенцијалних преступника да ће бити откривени и ухваћени, што би требало да их одврати од чињења преступа. Британски криминолози сматрају да системи видео-надзора могу значајно допринети превенцији криминала јер омогућавају: откривање учинилаца за време извршења кривичног дела или касније, редуковање времена током кога се може извршити кривично дело, појачавање природног надзора, унапређивање успешности физичког обезбеђења, јачање друштвене кохезије, подизање нивоа опрезности, појачавање страха од јавне срамоте, стимулисање кретања у подручјима покривеним видео-надзором и пораст броја пријављивања случајева полицији.

Министарство унутрашњих послова се определило за увођење нових техничких решења и система који прате најновије тенденције у развоју технологије како би се повећала безбедност грађана и допринело ефикаснијој борби против криминала, као и других појавних облика угрожавања друштва, по угледу на многе земље које користе тзв.интелигентни системи видео-надзора, а који се примењују широм света.Овакви системи се константно унапређују и показали су се као веома важни у раду полиције.

*Употреба сложених система видео-надзора у заштити приватног и јавног простора започела је крајем шездесетих година 20. века, како би се створили услови за*

сигурно улагање капитала и умањио страх од криминала путем редуковања стопе извршених кривичних дела на подручјима покривеним видео надзором. Прве камере у САД постављале су се у банкама, а у Великој Британији у малопродајним објектима. Иако се видео-надзор у почетку користио за осигуравање капитала, политичких и економских интереса, данас има далеко ширу употребу и представља значајно средство у контроли криминала од стране државе.

Према резултатима истраживања примене видео-надзора на јавним местима у седам европских земаља (Велика Британија, Шпанија, Мађарска, Аустрија, Немачка, Норвешка и Данска), судећи по распрострањености и технолошком квалитету примене, на првом месту налази се Велика Британија (40%), а на последњем Аустрија (18%) (Хемпел, То-пфер, 2004). Типичне локације за примену видео-надзора су железничке станице, подземне железнице и аеродроми, док се сасвим ретко надзиру факултети и цркве. Видео-надзор се често употребљава и у установама које се базе финансијама, амбасадама, музејима, болницама и друго. Уочене су знатне разлике у развоју уличног надзора међу различитим државама и градовима Европе. На пример, у Великој Британији 40000 камера покрива око 500 градова, у Немачкој мање од 100 камера покрива 15 градова, док Данска нема развијен улични систем видео-надзора<sup>1</sup>.

Како би Република Србија следила позитивне трендове и искуства других земаља покренут је пројекат „Safe city“ који подразумева увођење једног оваквог интелигентног видео-надзора. С тим у вези је планирано проширење видео-надзора Града Београда са више камерних места. Очекује се да ће се на овај начин постићи већа општа безбедност на територији града.

Предвиђено је планско формирање и увођење система видео-надзора Града Београда који ће се реализовати у више фаза. Такав јединствен систем ће помоћи у бржој детекцији опасности и њеном ефикаснијем отклањању, као и бржој размени информација.

Подаци који ће се прикупљати овим системом ће се користити искључиво и само у сврху остваривања безбедносне заштите живота, права и слобода грађана, заштите имовине, као и подршке владавини права.

Овим системом се већ постојећи послови и овлашћења полиције унапређују, и на тај начин се у знатној мери штеде пре свега људски и материјални ресурси. Мањом употребом људства, средстава и за краће време се постиже већи ефекат како у превентивном, тако и у репресивном смислу. Овакав систем је и те како битан за ефикасно прикупљање велике количне података и њихову евентуалну каснију употребу у складу са законом, а ради обављања поверених полицијских послова. Систем видео надзора града Београда је још увек у фази тестирања, међутим употреба видео надзора у раду полиције је већ дала резултате, тј. снимци са постојећих камера су у великој мери помогли полицији приликом обављања полицијских послова.

Оператери на постојећем систему видео-надзора су у више наврата, без претходне пријаве грађана уочавали саобраћајне незгоде на које су одмах упућивали патроле, а по потреби и остале службе (СХП, ватрогасце и др.) а све у циљу пружања неопходне помоћи повређеним лицима и омогућавања несметаног протока саобраћаја. Такође, су у више наврата уочили лица која су прескочила заштитне ограде на Бранковом и Панчевачком мосту у намери да изврше суицид и слањем и усмеравањем полицијских патрола успевали да спасу људске животе. У више наврата, од стране

оператера уочени су пожари на возилима и објектима, последице проузроковане временским непогодама, нарушавање јавног реда и мира приликом праћења јавних скупова, као и извршиоци кривичних дела, што им је омогућило правовремено упућивање полицијских службеника на лице места и усмеравање њиховог рада, а што је довело до хватања извршилаца прекршаја и кривичних дела.

Такође, полицијски службеници су у више наврата прегледом наснимљеног видео материјала уочили само кривично дело, као и правце доласка и одласка извршиоца кривичног дела, а такође је видео надзор помогао и у идентификовању предмета и трагова кривичног дела, што је допринело бржој идентификацији извршиоца и његовом проналаску.

Такође су у више наврата идентификована возила и лица која су учествовала у тешким саобраћајним незгодама, која су се удаљила са лица места.

Помоћу овог система извршиоци кривичног дела и прекршаја су у више наврата идентификовани много брже, уз уштеду људских, материјалних и других средстава.

#### 4.2. Предности коришћења видео-надзора

Предности коришћења видео-надзора:

- константан надзор над одређеном саобраћајницом;
- уштеда материјалних и људских ресурса;
- могућност контроле протока саобраћаја на местима на којима непосредна контрола од стране полицијских службеника није могућа;
- обезбеђење квалитетних доказа за вођење одговарајућих поступака;
- смањење ризика од корупције;
- постизање превентивног ефекта.

Приликом решавања кривичних дела и прекршаја у ранијем периоду полицијски службеници су се ослањали на снимке са видео-надзора друштвених фирми, институција, предузећа, физичких лица и других, и поред чињенице да се ради о системима видео надзора који су без контроле и надзора, а чија употреба је подложна злоупотребама од стране њихових ималаца. Ти појединачни видео надзори су у широкој примени годинама уназад и већина њих је углавном лошег квалитета, и као такви су функционисали без системских уређених права и обавеза руковоца наведеним системима. Коришћење видео записа са ових система је за полицију изузетно тешко, споро и захтева мноштво процедура за прибављање таквог материјала.

Полиција у свом раду, ради обављања полицијских послова, врши обраду података који су прикупљани применом полицијских мера и радњи, у складу са законом. Члан 47. ст. 2.т.5. Закона о полицији предвиђа између осталог, снимање на јавном месту, као посебну полицијску меру и радњу.

На овај начин се не проширују полицијска овлашћења, односно не уводе се никакве нове мере и радње које до сада нису примењиване, већ се ради о полицијским мерама које се стално унапређују и уређују законом. Широка примена сваремене

технолије од стране криминалаца условљава и полицију да прати трендове и законом предвиђене мере и радње обавља такође употребом савремених технологија, као што је и систем интелигентног видео надзора.

Само снимање на јавном месту од стране полиције не представља повреду, права и слобода лица јер се ради о легитимним активностима полиције те се самим тим не може говорити о угрожавању приватност лица. Приликом сваке даље обраде видео материјала (нпр. преглед и анализа видео записа ради откривања кривичног дела, извршиоца и сл.) не може се говорити о угрожавању права и слобода лица која се случајно односно стицајем околности затекну на месту догађаја и на простору који је покривен видео надзором. Министарство унутрашњих послова је такав вид угрожавања приватности препознало као ризик у употреби видео надзора, те је Упутством о условима изградње, коришћења о одржавња система видео надзора Републике Србије прописало мере заштите података о лицима која нису предмет полицијске обраде, а у складу са Законом о заштити података о личности.

#### 4.3. Утицај људског фактора на употребу система видео-надзора

Као и у свим другим системима где је немогуће искључити улогу човека који на било који начин рукује технологијом тако је немогуће стопроцентно искључити тзв. људски фактор као потенцијални ризик за угрожавање права грађана. Немогуће је утицати на свест сваког овлашћеног обрађивача података и апсолутно спречити неовлашћену, несавесну и злонамерну употребу прикупљених података приликом обраде.

С тим у вези, Министарство унутрашњих послове је људски фактор у употреби интелигентног система видео надзора препознало као највећи ризик по права и слободу лица чији се подаци обрађују (лица која су обухваћена видео записима). Важећом Обавезном инструкцијом о одржавању и коришћењу система видео надзора у Републици Србији прописане су процедуре у раду са прикупљеним подацима, тј. процедуре обраде података, а Упутством о условима изградње, коришћења о одржавња система видео надзора Републике Србије и Упутством о јединственом начину вођења евиденција у области видео акустичког снимања, који су у изради наведене процедуре ће бити детаљно објашњене, а све у циљу смањивања могућности злоупотреба на најмању могућу меру.

Законом о полицији прописане су санкције, тј. одговорност за евентуалне злоупотребе и повреде службене дужности од стране запослених. Санкционисање полицијских службеника који евентуално злоупотребе своја овлашћења приликом обраде података предвиђено је и другим законима. (Кривични законик чл. 143)

Осим примарне намене система видео надзора као што је општа сигурност грађана, систем представља и један моћан вид контроле рада полицијских службеника, јер омогућава увид у законитост поступања односно рада полиције. На овај начин систем видео надзора улива додатну сигурности грађана у законито поступање полиције.

## 5. Хронологија увођења интегрисаног система видео-надзора

### 5.1. Спровођење пројекта „Сигурно друштво“ од стране МУП-А

Министарство унутрашњих послова и компанија „Huawei Technologies Co, Ltd“ су 2011. године започели разговоре о могућностима и унапређењима информационог и телекомуникационог система Министарства унутрашњих послова кроз израду решења за повећање опште безбедности грађана кроз пројекат „Сигурно друштво“, под окриљем претходно закљученог Споразума о економској и техничкој сарадњи у области инфраструктуре између Владе Републике Србије и Владе Републике Кине који је потписан у Пекингу, НР Кина дана 20.08.2009. године (потврђено Законом о потврђивању Споразума о економској и техничкој сарадњи у области инфраструктуре између Владе Републике Србије и Владе Републике Кине, „Сл. гласник РС – Међународни уговори“, број 90/2013, 9/2013 – др. Закон и 13/2013 – др. закон).

Дана 17.12.2014. године, у Београду је између Министарства унутрашњих послова и компаније „Huawei Technologies Co, Ltd“ закључен Меморандум о разумевању који се односи на предложену сарадњу и кораке које је потребно предузети у погледу реализације пројекта „Сигурно друштво“.

На основу наведеног Споразума о економској и техничкој сарадњи у области инфраструктуре између Владе Републике Србије и Владе Републике Кине, као и на основу наведеног Меморандума о разумевању, дана 7.2.2017. године закључен је Споразум о стратешком партнерству за увођење eLTE технологија и решења за „безбедан град“ у системима јавне безбедности између Министарства унутрашњих послова и Компаније „Huawei Technologies Co, Ltd“. На овај споразум Влада Републике Србије је претходно дала сагласност Закључком 05 број 337-12737/16 од 29.12.2016. год.

Закључком Владе Републике Србије П 05 број: 00-109/2017. од 19.05.2017. год. дата је сагласност да Министарство унутрашњих послова закључи уговор о имплементацији капиталног пројекта „Видео надзор у саобраћају – Фаза I“ са компанијом Huawei Technologies Co. Ltd.

Капиталним пројектом „Видео надзор у саобраћају – Фаза I“ у току 2017. год. Министарство унутрашњих послова реализовало је реконструкцију дотадашњег видео надзора града Београда, као и реконструкцију Командно-оперативног центра ПУ за град Београд где је смештен „data center“ система и главни кориснички центар Дежурне службе ПУ за град Београд.

Реконструкцијом система видео надзора, на 61 локацији у граду, постављено је преко 100 камера и инсталиран „интелигентан“ систем видео надзора, који поред амбијенталног, односно, панорамног видео надзора простора, обухвата и видео аналитику добијених сигнала. Овакав систем омогућава анализу тренутних и протеклих дешавања значајних за расветљавање кризних ситуација по различитим критеријумима (објекту, возилу, таблици, понашању, боји и др.).

Пројекат „Видео надзор у саобраћају-фаза 1“ МУП-а Републике Србије обухватио је:

- Реконструкцију Командно оперативног центра ПУ за град Београд
- Инсталацију „паметних“ камера напредне технологије и карактеристика на 61 камерном месту у граду, и то 59 покретних камера и 47 фиксних камера високе резолуције
- Набавку опреме и њену инсталацију у КОЦ-у: сервера, инфраструктуре и опреме за архивирање сигнала
- Набавку и инсталацију софтвера за администрацију и управљање системом и напредну видео аналитику кроз анализе као што су:

Анализа дешавања у зони надзора камере: у реалном времену детектовање догађаја као што су остављање/померање или напуштање неког објекта, повећан број људи на неком простору, улазак у дефинисану зону, задржавање у дефинисаној зони током неког периода времена, уочавање погрешног смера кретања, бројање људи и др.

Видео претраживање: интелигентна претрага видео материјала према различитим задатим критеријумима: простору, времену, дешавању на сцени, објекту и типу објекта (возило, човек, предмет), боји објекта, зони на сцени, смеру кретања

Видео синопсис: сажет приказ видео материјала

Препознавање регистарских таблица моторних возила: препознавање таблица моторних возила у реалном времену и претрагом снимљеног материјала

- Инсталацију видео зидова
- Реконструкцију постојеће телекомуникационе мреже пребацивањем на систем специјалних веза (ССВ) мрежу органа одбране и безбедности Републике Србије.
- Опремање три Дежурне службе Полицијских станица Нови Београд, Стари град и Савски венац опремом за приступ систему и праћење сигнала са камера.
- Набавку и инсталацију радних станица оператера за праћење и интелигентну видео аналитику сигнала са система.

Капиталним пројектом „Видео надзор у саобраћају – Фаза 2“, наставља се реализација пројекта „Безбедан град“ на целокупној територији града Београда. Предвиђено је да се на више 800 нових локација (камерних места) поставе камере, при чему ће се реализација пројекта вршити у фазама, у укупном трајању од три године.

Имајући у виду да су првом фазом пројекта „Безбедан град“ постављени темељи комплетног система и дефинисани правци у којима ће се кретати приликом реализације целокупног пројекта, фаза два представља надоградњу започетог система са додатним проширењем територијалне покривености града системима видео надзора, као и проширење функционалности тих система.

Задатак пројекта „Видео надзор у саобраћају – Фаза 2“ је покривање читавог града Београда (17 општина), као и проширење функционалности аналитике видео материјала следећим алатима:

- Препознавање лица - AFR (Automatic Face Recognition )
- Интеграција са GIS-платформом – праћење трајекторије возила,

као и, евентуално, увођењем система за аутоматско препознавање регистарских таблица и детекцију саобраћајних прекршаја моторних возила.

Постојећи, „Интелигентни“ систем видео надзора ће се даље надоградити и проширити, како новим локацијама камерних места, тако и увођењем нових функционалности видео аналитике. Проширење броја камерних места биће праћено адекватним проширењем „Data center“-а свим потребним хардверским компонентама, унапређеним софтверским верзијама система и повећањем броја лиценци за напредну аналитику видео сигнала. Такође, пројекат обухвата и опремање Дежурних служби полицијских станица по општинама, опремом за приступ систему и праћење сигнала са камера.

Одабир безбедносно интересантних локација, за постављање камера, врше оперативне јединице Министарства унутрашњих послова: Управа полиције, Управа криминалистичке полиције, Управа саобраћајне полиције, Јединица за заштиту одређених објеката.

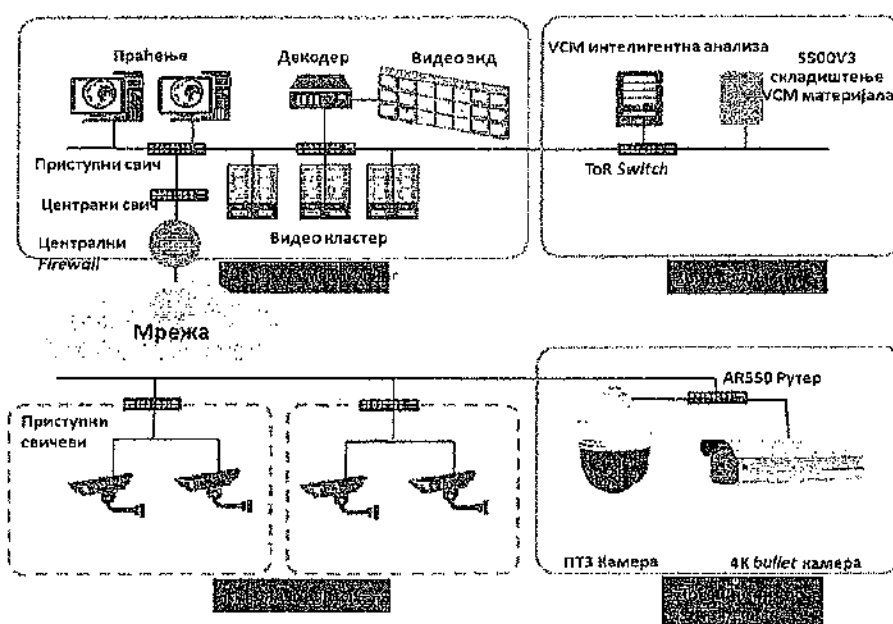
## 5.2. Опис система видео надзора

Систем интелигентног видео надзора – IVS је систем који се састоји од две компоненте:

- Систем видео надзора опште намене
- Интелигентна видео аналитика

Систем се састоји од камерних места, локалне приступне мреже, транспортне мреже, уређаја за администрацију и управљање системом, уређаја за интелигентну видео аналитику, система за складиштење видео материјала са камера, система за складиштење резултата аналитике, корисничких центара за преглед камера и снимљеног материјала, корисничког центра за напредну претрагу сигнала са камера и снимљеног видео материјала употребом алата видео аналитике и уређаја за резервно напајање.

Слика 1. Архитектура система видео надзора



Покретне (PTZ) камере су резолуције fullHD (2Mpix) са 30x оптичким зумом, фиксне камере су резолуције fullHD (2Mpix) осим фиксних камера које су намењене за препознавање регистарских таблица постављених током фазе 1 су у резолуцији 4K (8Mpix). Све камере су опремљене са IR диодама чиме им је омогућен рад у ноћним условима.

Камере имају слот за картице који се користи као backup за снимање у случајевима када дође до прекида у преносном/комуникационом путу од камере до сервера на коме се, у нормалном режиму рада, снима видео сигнал са камера. Фиксне камере долазе са моторизованим варифокалним објективом који пружа могућност да се подеси видно поље камере. Видно поље камере условљено је врстом објектива који се користи. Користи се софтвер компаније „Huawei“.

Телекомуникациона мрежа, преко које се реализује систем видео надзора, је сасвим независна мрежа, која нема додирних тачака са јавном мрежом, а поготову не са Интернетом. Администрацију мреже раде надлежни радници МУП-а Републике Србије и приступ је строго рестриктиван са рачунара који су опредељени само за ту намену. Сваки покушај повезивања на ту мрежу мимо процедуре се детектује, укључује се аларм на који надлежни радници МУП-а реагују.

Уређаја за администрацију и управљање системом (VCN), уређаја за интелигентну видео аналитику (VCM), система за складиштење видео материјала са камера, система за складиштење резултата аналитике и остала мрежна опрема (switch-еви, firewall-ови, router-и сл.) налазе у „Data centru“ у систем сали КОЦ, ПУ за град Београд која је покривена системом видео надзора. Приступ систем сали имају представници техничке службе Министарства.

Мере заштите су следеће: заштита на нивоу мреже, техничка заштита (видео надзор), праћењем рада корисника кроз логове, мере противпожарне заштите, заштита од поплава, односно, сви видови заштите које сервер сала мора да испуни.

Систем за складиштење видео материјала са камера и систем за складиштење резултата аналитике, односно, storage на коме се чува снимљени видео материјал са камера и storage за снимање резултата видео аналитике налазе се на уређајима који су део Data Centar-а и део су већ поменуте, изоловане мреже МУП-а, која је додатно опремљена „firewall“ уређајем помоћу кога се додатно обавља контрола приступа и комуникације између уређаја у мрежи. Уређаји за администрацију и управљање системом (VCN), уређаја за интелигентну видео аналитику (VCM), система за складиштење видео материјала са камера и система за складиштење резултата аналитике, поред поменутих заштитних мера на мрежном нивоу, имају организован систем приступа кроз дефинисање корисничких рола са различитим нивоом приступа систему, односно, приликом приступа систему видео надзора корисник мора имати кориснички налог и шифру. Поред свега наведеног, уређаји имају и резервисан део за складиштење логова корисника (кад је неко приступио систему, шта је радио на систему и слично).

Снимци са камера се чувају у складу са роковима предвиђеним у Закону о евиденцији и обради података у области унутрашњих послова.

Софтвер за видео менаџмент и управљање који се користи је софтвер фирме „Huawei“ који је још у фази прилагођавања захтевима Министарства, односно фирма „Huawei“ ради на унапређењу како функционалности софтвера тако и на карактеристикама које захтевају што транспаретнију и бољу заштиту информација добијених применом аналитичких алата. У току је реализација софтверског пакета, од стране фирме „Huawei“ који би омогућио криптовање, односно, заштиту од „edit“-овања резултата аналитика.

Мониторинг центар кога чини опрема за праћење сигнала у реалном времену са система видео надзора у Београду, налази се у просторијама ПУ за град Београд, у Булевару деспота Стефана 107, као и у простојима ПС Савски венац, Стари град и Нови Београд.

### 5.3. Администрација системом видео надзора

Системом администрирају представници техничке службе Министарства, односно Сектора за аналитику, телекомуникационе и информационе технологије. Поступање се обавља према Обавезној инструкцији о одржавању и коришћењу система видео надзора у Републици Србији и према Обавезној инструкцији о одржавању и коришћењу градских раскрсница и саобраћајница у Београду, с тим да је у припреми ново Упутство о условима изградње, коришћења и одржавања система видео надзора у Министарству унутрашњих послова.

У оквиру наведеног документа предвиђено је следеће:

- Сектор за аналитику, телекомуникационе и информационе технологије (у даљем тексту САТИТ) ће водити евиденцију о свим постојећим системима видео надзора које Министарство користи, а који обавезно мора да садржи: опис свих камерних места са прецизном локацијом и идентификационом ознаком камере, опис свих корисничких центара са подацима о руковооцима и корисницима система видео надзора.
- САТИТ ће евидентирати и ажурирати све додељене приступне шифре и лозинке са нивоима приступа овлашћеним оператерима и администраторима, са називима радних места, у сарадњи са организационом јединицом \_ корисником система видео надзора.
- Снимање – чување (складиштење) података прикупљених системом видео надзора Министарства врши се аутоматски на носачима податка (на медијима за чување података) у систему видео надзора Министарства, без системског преноса на спољне медије (осим у случају нарушавања јавног реда и мира, ванредних ситуација и сл. из тачке 27. овог упутства).
- Заштита података је обезбеђена на начин да приступ складиштеним подацима имају администратори и корисници система, у складу са одобреним нивоом приступа.
- Администратори система видео надзора су представници САТИТ у полицијској управи којој територијално припада систем. Начелник САТИТ или лице које он

овласти одобрава администраторске нивое односно, ниво администрације система и приступа подацима.

- Оператере и кориснике система опредељује организациона јединица која је надлежна за управљање системом видео надзора и одређује оператере и нивое приступа и поступања са подацима.

Такође, у току је израда текста Упутство о јединственом начину вођења евиденција у области видео акустичког снимања којим се ближе уређује начин вођења евиденција у области видео-акустичког снимања у Министарству унутрашњих послова и чиме су обухваћене следеће ставке:

- Видео записи добијени употребом камера система за видео-акустичко снимање садрже назив и локацију камере и временску линију снимљених догађаја и чувају се на систему локално, аутоматски, у електронској форми на носачима податка (на медијима за чување података), без системског преноса на спољне медије.
- Евиденција материјала за обраду садржи видео-аудио записе, фотографије и алфанумеричке податке (регистарске ознаке возила, тип и боја возила или објекта, лични опис лица, кључне речи). Евиденција материјала за обраду може да садржи и друге податке који нису подаци о личности.
- Евиденција материјала за обраду води се на систему локално, кроз програмску апликацију система видео надзора, у електронској форми на носачима податка (на медијима за чување података), без системског преноса на спољне медије.
- Евиденције обрађеног материјала су резултати видео аналитике и садрже видео и аудио записе, фотографије догађаја, простора, лица и возила, алфанумеричке податке, време догађаја, датум догађаја, назив и локацију камере, личне податке о лицима, регистарске ознаке возила, тип возила, боју возила или објекта, лични опис лица, податке о возилу, податке о власнику возила, ЈМБГ, податке о прекршају. Евиденције обрађеног материјала могу да садрже и друге податке који нису подаци о личности.
- Евиденције обрађеног материјала чувају се на систему локално, аутоматски, у електронској форми на носачима податка (на медијима за чување података), без системског преноса на спољне медије.
- Евиденције о корисницима и администраторима система видео надзора садрже име и презиме, корисничко име на систему, ЈМБГ, назив организационе јединице, назив радног места, датум и време доделе права приступа, датум и време укидања права приступа.
- Евиденције о корисницима и администраторима система видео надзора, воде се локално, кроз програмску апликацију система видео надзора, у електронској форми на носачима податка (на медијима за чување података) у систему видео надзора, без системског преноса на спољне медије.

- Евиденције о приступу и коришћењу, односно о активностима и трансакцијама на систему су тзв. „логови“ на систему и садрже датум и време активности, врсту активности, корисничко име налога који је спровео активност, „IP“ адресу рачунара са којег је извршена активност.
- Евиденције о приступу и коришћењу, односно о активностима и трансакцијама на систему чувају се на систему локално, аутоматски, у електронској форми на носачима податка (на медијима за чување података), без системског преноса на спољне медије.
- Евиденција захтева за креирање или укидање корисничких налога за приступ и коришћење система садржи: назив организационе јединице која захтева приступ систему, број захтева, идентификацију система за видео-акустичко снимање, име и презиме полицијског службеника или другог овлашћеног лица које предузима захтеване радње, ЈМБГ, назив радног места, опис извршене радње обраде на систему, име и презиме креираног корисника, корисничко име на систему, ЈМБГ, назив организационе јединице, назив радног места, ниво права приступа, датум и време доделе права приступа, датум и време укидања права приступа.
- Евиденција захтева за креирање или укидање корисничких налога за приступ и коришћење система се води ручно, електронски, у облику табеле на обрасцу бр 1, која је саставни део овог Упутства.
- У сваком корисничком центру води се евиденција о сваком захтеву за изузимање, прегледање, аналитику видео материјала, унос материјала за обраду, копирање и умножавање видео и аудио записа и резултата обрађеног материјала (интелигентна видео аналитика) , која садржи: назив организационе јединице која захтева радњу на систему, број захтева, идентификацију система за видео-акустичко снимање, име и презиме полицијског службеника или другог овлашћеног лица које предузима захтеване радње обраде, ЈМБГ, број службене легитимације, опис извршене радње обраде на систему (прегледање видео материјала, унос материјала за обраду, врста интелигентне видео аналитике, изузимање, копирање и умножавање видео или аудио записа или резултата видео аналитике), податке о предатом материјалу за обраду (фотографија, алфанумерички податак, видео запис), податке за идентификацију видео и аудио записа или резултата видео аналитике (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, тип података резултата видео аналитике), број направљених копија.
- Евиденција о сваком захтеву за изузимање, прегледање, аналитику видео материјала, унос материјала за обраду, копирање и умножавање видео и аудио записа и резултата обрађеног материјала (интелигентна видео аналитика) се води локално, ручно, електронски, у облику табеле на обрасцу бр.2, која је саставни део овог Упутства.
- Непосредно након преноса – копирања података на спољне медије, корисник који је извршио копирање у обавези је да предметни видео-запис уклони

брисањем са локалног меморијског простора радне станице или било које друге привремене меморијске локације.

- Сектор надлежан за аналитику, телекомуникационе и информационе технологије (у даљем тексту: САТИТ) води евиденције о свим постојећим системима за видео акустичко снимање које Министарство користи, а које садрже: идентификацију система за видео-акустичко снимање, податке о руковооцима система видео надзора (организациона јединица Министарства или други орган/правно лице), идентификационе податке о одлуци о изградњи/набавци опреме за систем или надоградњи постојећег система Министарства или о споразуму о уступању Министарству система развијеног од стране другог органа/правног лица.
- Евиденције о свим постојећим системима за видео и акустичко снимање се воде локално, ручно, електронски, у облику табеле на обрасцу бр 3, који је саставни део овог Упутства.
- Корисници система за видео акустичко снимање имају различите нивое приступа систему:
  - основни ниво корисника – има могућност праћења видео сигнала са камера у реалном времену
  - средњи ниво корисника – има могућност праћења видео сигнала са камера у реалном времену и прегледа снимљеног (складиштеног) материјала
  - виши ниво корисника – има могућност праћења видео сигнала са камера у реалном времену, прегледа снимљеног материјала и копирања снимљеног материјала на спољне преносне медијуме.
  - корисник алата видео аналитике – има могућност коришћења напредних аналитичких алата за обраду видео сигнала са камера према креираним захтевима за аналитиком
  - виши корисник алата видео аналитике – има могућност дефинисања захтева за аналитиком видео сигнала и копирања резултата аналитике на спољне преносне медијуме.
- Корисници система приступају систему видео надзора кроз корисничке апликације система.
- Администратори система – врше администрацију система и креирање и администрацију корисничких налога.
- Администратори система приступају систему видео надзора кроз корисничке и системске апликације система.
- Администратори система видео надзора су представници САТИТ у полицијској управи којој територијално припада систем. Начелник САТИТ или лице које он овласти одобрава администраторске нивое, односно, ниво администрације система и приступа подацима.
- Системом видео надзора управља надлежна организациона јединица на основу одлуке о изградњи/набавци опреме за систем или надоградњи постојећег

система Министарства или о споразуму о уступању Министарству система развијеног од стране другог органа/правног лица коју је донео/закључио министар или лице које он овласти

- Корисници система видео надзора су припадници организационе јединице надлежне за систем. Кориснике и нивое приступа корисника система видео надзора у оквиру организационе јединице надлежне за систем одређује руководилац надлежне организационе јединице.
- Организационе јединице које одлуком о његовом увођењу нису опредељене као корисници, захтев за приступ систему видео надзора, са образложењем и нивоима приступа, подносе Кабинету министра или Дирекцији полиције.
- Заштита података на системима за видео акустичко снимање је обезбеђена на начин да приступ складиштеним подацима имају администратори и корисници система, корисничким именом и приступном шифром, у складу са одобреним нивоом приступа.
- Мере заштите података у корисничким центрима које се могу огледати у ограничењу употребе комуникационих средстава (снимање видео записа мобилним телефоном, неовлашћен пренос података на други носач - УСБ, ЦД и др) и контроли приступа предузима, спроводи и за њих одговара руководилац те организационе јединице.
- Овлашћени радници организационих јединица Министарства, који формирају евиденције, одговорни су за тачност, потпуност, исправност и ажурност података.
- Контролу вођења евиденција, односно њене тачности, потпуности, исправности и ажурности података обезбеђују руководиоци организационих јединица Министарства које воде евиденцију.

## Закључак

Примена видео-надзора регулисана је законским и подзаконским актима, али и документима међународног карактера који се односе на заштиту података о личности, рад полиције, кривични поступак, посебним законима о видео-надзору и другим прописима којима се регулише безбедност на појединим локацијама (нпр. банке, стадиони и др.). Прописи на европском нивоу углавном регулишу питања заштите приватности и поступања са подацима који су прикупљени путем видео- надзора. У том погледу, посебну важност имају Европска конвенција за заштиту људских права и основних слобода, Европска конвенција о заштити лица у односу на аутоматску обраду личних података и Уредба (EU) 2016/679 Европског парламента и Савета о заштити појединаца у вези са обрадом података о личности и слободном протоку таквих података те о стављању ван снаге Директиве 95/46 и Директивом (EU) 2016/680 Европског парламента и Савета о заштити појединаца у вези с обрадом података о личности од стране надлежних органа у сврхе спречавања, истраге, или откривања кривичних дела или извршавања кривичних санкција и о слободном преносу таквих података те о стављању ван снаге Оквирне одлуке Савета 2008/977/ПУП

*Као резултат политичког притиска да се национална законодавства ускладе са европским стандардима, европске државе изнедриле су различите прописе како би регулисале област примене видео-надзора. Тако Велика Британија, између осталих прописа, има посебан правилник о примени видео-надзора који је дат од стране*

*Повереника за заштиту информација, Шпанија инструкције о видео-надзору служби безбедности у јавном простору, Данска правилник којим се строго забрањује надзирање јавних простора од стране приватних компанија и на друге начине ограничава примена видео-надзора. Неке државе, као што су Немачка, Луксембург, Белгија, Финска, Грчка и Италија, допуниле су постојеће законе о заштити података о личности одредбама које се односе на видео-надзор. Новим законским одредбама одређују се сврха и услови примене видео-надзора, начин информисања грађана, квалитет видео-записа, чување и процесуирање података и друго. У складу са начелом транспарентности, Норвешка, Француска и Шведска увеле су процедуре за регистровање система за видео-надзор".*

И у законодавство Републике Србије уведене су иновације које се тичу примене видео-надзора. Законом о заштити података о личности уређују се услови за прикупљање и обраду података о личности, права лица и заштита права лица чији се подаци прикупљају и обрађују, ограничења заштите података о личности, поступак пред надлежним органом за заштиту података о личности, обезбеђење података, евиденција, изношење података из Републике Србије и надзор над извршавањем овог Закона. Према мишљењу Повереника за информације од јавног значаја и заштиту података о личности Републике Србије, кључни недостатак новог Закона представља недостатак одредби које се тичу видео-надзора (Извештај Повереника, 2012). Стога је по његовом мишљењу потребно изградити посебан закон о видео-надзору или је у нови Закон о заштити података о личности требало унети одредбе којима се детаљније регулише примена видео-надзора као што је предвиђено и Стратегијом заштите података о личности.

Могући негативни аспекти примене видео надзора

*Ефективност видео-надзора у превенцији криминала директно зависи од тога да ли су потенцијални преступници свесни да се њихово понашање прати и да на овај начин могу бити откривени и ухапшени. Због тога, савремени аутори сматрају да видео-надзор представља репресивно, а не превентивно оруђе, односно да може имати превентивну улогу само уколико су особе биле свесне постављаног видео-надзора. Међутим, савремена истраживања показују да грађани углавном не знају када се њихово понашање прати. То потврђују и резултати истраживања рађеног у Глазгову, према којима је три месеца након постављања видео-надзора на градским улицама само 33% грађана тога било свесно, а 15 месеци након инсталације 41% грађана. Уколико се изузме 6-7% оних који су знали да су улице под видео-надзором, али не и да ли на месту на коме су интервјуисани има камера, може се рећи да је само четвртина грађана након три месеца од примене видео-надзора била свесна постојања видео-надзора, а трећина након 15 месеци. При томе, показало се да је млађа популација свеснија постојања камера, као и они који се чешће крећу по градским улицама.*

*Окружење у коме се криминал данас испољава, захтева и промену приступа у контроли криминала. Значајне промене у вршењу и друштвеној реакцији на криминал настале су услед ратидног развоја технологије. Технологија се данас сматра битним оруђем у вршењу криминала. При реаговању на криминал уз употребу технологија предност се даје унапређивању праксе превентивног поступања, много мање*

санкционисању и третману. Данас у ту сврху користе се биометријске технологије, видео надзор, технологије за надзор над комуникацијама и друго. Конвенционалној криминологији супротставља се такозвана "наука о криминалу" која мора бити много применљивија, са акцентом на разумевање криминала уместо криминалаца, моменталну редукцију криминала уместо дуготрајне социјалне реформе, редуковање штете нанете жртвама уместо помагања криминалцима, проблемски уместо теоријски оријентисана, усмерена промени политике у контроли криминала. Годинама уназад овај приступ препознат је као успешан у превенцији и редуковању криминала на специфичним местима (аеродроми, гранични прелази, јавни превоз, школе, затвори, улице).

Глобално ширење утицаја капитализма и индустријализације, посебно развој војне индустрије, доприносе убрзаном развоју безбедносних технологија у циљу унапређивања контроле и надзора модерног друштва.

Намећу се питања у којој мери су ризици, онако како их данас перципирамо, продуктовани и који су прави домети прокламоване бриге за безбедност грађана и унапређивања националне сигурности држава. Аутори се слажу да у данашњем друштву, популарно названом друштву ризика, људи у великој мери живе живот са "страхом као погледом на свет". Иако је реч ризик првобитно могла да има и позитивно и негативно значење, у актуелним друштвеним приликама најчешће се своди на синоним за опасност. Према томе, нико није безбедан, без обзира на друштвени статус и друге разлике. Аутори разматрају тезу о градовима као изворима страха који су првобитно подизани да заштите становнике од спољних опасности. Грађанима су на располагању различите технологије које би требало да их заштите, али и обезбеђују праћење и надзор различитих аспеката њиховог живота, па је како (Свенсен) примећује надзирање грађана интензивније и екстензивније него икада раније и све већи део приватних живота постаје видљив за невидљиве посматраче. Међутим, питање је колико је својеврсна жртва приватности прихватљива грађанима и колико су технологије по себи ризичне. Кларк је још седамдесетих година предвидео друштво у коме нико неће знати да ли се сваки његов покрет посматра, свака реч слуша, или ће пак сви знати да је то тако, али је извесно да нико неће видети никакво зло у томе.

Замерке које се често упућују на рачун примене видео-надзора тичу се угрожавања приватности и злоупотребе ове мере у политичке и комерцијалне сврхе. Савремена истраживања потврђују да грађани препознају и не оправдавају манипулисање њиховим страхом од криминала. У студији која је рађена у Шпанији откривено је да грађани дово- де у питање критеријуме одређивања проблематичног понашања које ће се пратити путем видео-надзора и да сматрају да постоје људска и техничка ограничења која омогућавају злоупотребу података који су прикупљени на овај начин. Према ауторима ове студије, грађани су указали на потребу за „бољом“ сигурношћу, а не за „више“ сигурности. Другим речима, јавност је сагласна са применом видео- надзора у контроли криминала, али само када је то неопходно и уз дефинисање услова којима ће се заштитити приватност појединца.

Полазећи од традиционалне идеје да је надзор ауторитаран одговор на неконформизам, при чему се искљученост користи као доминантна стратегија контроле, неки аутори износе примедбу да видео-надзор подстиче социјалну искљученост. Према Ломелу, у тржном центру у Ослу у Норвешкој пажњу оперативаца су привлачили људи запуштеног изгледа, пре него они који су вршили

криминалне радње. Према томе, системи видео-надзора су подешени тако да се лакше региструју непожељне особе, као што су просјаци, улични продавци, бескућници и друге маргинализоване групе. Такође, може се чути и мишљење да се овим путем подстичу расизам и сексизам. Сматра се да је један и по до два и по пута извесније да ће Афроамериканци бити подвргнути детаљнијем надзору од стране оператера него припадници других раса. Зато, треба настојати да се даљом аутоматизацијом система видео-надзора овакви проблеми ублаже.

Иако би видео-надзор, у савременом смислу речи, требало да представља проактивну технологију, то није увек случај. Постоје значајне разлике у односу на технолошку софистицираност и организационе капацитете установе или окружење у коме се примењује. Истраживањем квалитета система јавног надзора у Лондону у четири различита контекста утврђено је да се две трећине постојећих система ослања на фиксне камере, без дигиталног снимка и могућности за компјутерску обраду слике, што значајно умањује проактивну улогу надзора. Такође, ово истраживање је показало да већина службеника који се баве праћењем снимака, поред надзора, има и друга задужења, па се без обзира на њихове компетенције не може тврдити да ће пажљиво посматрати дешавања на екрану.

На крају, видео-надзор може изазвати географско, тактичко и методолошко измештање криминала, смањити ниво личне опрезности, моралне одговорности и самоконтроле грађана, као и изазвати губитак поверења у полицију.

Видео-надзор представља сложен социо-економски и културни феномен, са значајним потенцијалом за контролу криминала. Реч је о снажном оруђу контроле појединаца и друштвених група, које се развијало под окриљем ситуационе превенције, али и стратегији нулте толеранције, проблемски оријентисаном приступу и превенцији у заједници. Неки савремени аутори ситуациону превенцију оцењују као прагматични, аморални (или бар морално неутрални), технолошки, технократски, аполитични и инструментално рационални приступ. У складу са тим, видео-надзор се сматра ефективном мером превенције, а позитивна дејства приписују се ефекту застрашивања и позитивном психолошком деловању на појединце и заједнице.

Данас се видео-надзор користи у обезбеђивању функционисања различитих социјалних контекста, међу којима су јавни простори, школе и затвори. Истовремено, научна литература оскудева у радовима о делотворности видео-надзора, а резултати малобројних истраживања су прилично неусаглашени и међусобно неупоредиви. Услед помањкања квалитетних евалуација, тешко је дати коначан суд о ефективности примене видео-надзора и формулисати смернице за унапређивање праксе у овој области.

Ипак, на основу досадашњих емпиријских истраживања и практичних искустава могу се издвојити неке начелне препоруке за унапређивање примене и ефективности видео-надзора, а то су:

- видео- надзор примењивати само када је то неопходно и у складу са претходно утврђеном сврхом примене;
- врсту и трајање надзора ускладити са сврхом примене;
- информисати грађане о примени видео-надзора путем истицања јасних обавештења; прописати стандарде за осигуравање квалитета видео-записа;

•прописати процедуре за поступање са подацима који су прикупљени путем видео-надзора; максимално аутоматизовање и индивидуализовање видео-надзора;

•увођење регистра система за видео-надзор на локалном и републичком нивоу; унапређивање свести грађана о примени видео-надзора;

•унапређивање научних сазнања о примени видео-надзора, укључујући и спровођење методолошки квалитетних евалуација<sup>III</sup>.

Министарство унутршњих послова налази да у оквиру постојеће законске регулативе и доношењем одређених подзаконских аката употреба савременог видео надзора са моћним алатима видео аналитике може у значајној мери повећати сигурност грађана и да је с друге стране ризике по угрожавање права и слобода грађана могуће свести на минималну меру.

Такође ваљаном едукацијом запослених у Министарству и подизањем свести о неопходности заштите података о личности па и ефикаснијим санкционисањем за учињене пропусте у раду могуће је и највећи ризик по евентуално угрожавање права грађана који се по процени министарства огледа у људском фактору, свести на најмању могућу меру.

Проценом утицаја обраде на заштиту података о личности коришћењем система видео-надзора дошло се до закључка да је корист која се остварује употребом система видеа надзора много већа од евентуалних негативних последица по заштиту права грађана односно угрожавање података о личности која се штите законом где је уз примену препоруке за унапређивање примене и ефективности видео-надзора, мера задирања у приватност сведена на минимум, и на тај начин се може остварити сразмерност у обради података.

<sup>I</sup> Марина Ковачевић – Лепојевић, Весна Жунић – Павловић: Универзитет у Београду -Факултет за специјалну едукацију и рехабилитацију, "ПРИМЕНА ВИДЕО-НАДЗОРА У КОНТРОЛИ КРИМИНАЛА"

<sup>II</sup> Марина Ковачевић – Лепојевић, Весна Жунић – Павловић: Универзитет у Београду -Факултет за специјалну едукацију и рехабилитацију, "ПРИМЕНА ВИДЕО-НАДЗОРА У КОНТРОЛИ КРИМИНАЛА"

<sup>III</sup> Марина Ковачевић – Лепојевић, Весна Жунић – Павловић: Универзитет у Београду -Факултет за специјалну едукацију и рехабилитацију, "ПРИМЕНА ВИДЕО-НАДЗОРА У КОНТРОЛИ КРИМИНАЛА"

Београд 20. септембар 2019  
Бр. 01-1275/19-3



ПОТПРЕДСЕДНИК ВЛАДЕ И  
МИНИСТАР УНУТРАШЊИХ ПОСЛОВА  
*Nebojsa Stefanovic*  
др Небојша Стефановић