УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

Правни аспекти повреде података о личности у Републици Србији

(мастер рад)

Ментор:
Проф. др Дејан Вучетић

Студент:
Наташа Вуковић
Број индекса: М007/23-ИТ

Ниш, 2025.

САДРЖАЈ

I УВОД

У данашње доба убрзаног развоја дигиталних технологија заштита података о личности постаје један од највећих изазова, како за појединце, тако и за правне системе широм света. Честа кршења приватности грађана, било због злоупотребе података или због недовољно ефикасне контроле, све више утичу на безбедност грађана. У Србији, ова област правно је уређена Законом о заштити података о личности, који служи као кључни механизам за спречавање злоупотребе података о личности. Ипак, у пракси се сусрећемо са изазовима у примени закона, док нове технологије, попут вештачке интелигенције, додатно отежавају ситуацију и захтевају дубљу анализу и иновативан приступ у нормативном регулисању ове области.

Овај рад има за циљ да истражи правни оквир заштите података о личности у Републици Србији, анализира проблеме повреде података, као и да понуди предлоге за превенцију и управљање инцидентима. Тема је изабрана због њеног значаја у савременом друштву, али и због актуелности проблема који су све присутнији у пракси.

Предмет истраживања рада је правна анализа повреде података о личности, са посебним освртом на превенцију, управљање инцидентима и ризике примене нових технологија попут вештачке интелигенције у обради података о личности.

Циљ истраживања је процена ефикасности постојећег правног оквира у Републици Србији у погледу заштите података о личности и спречавању њихових повреда. Истовремено, рад настоји да идентификује кључне изазове у примени прописа који се односе на повреде података о личности, као и да истражи последице ових повреда на појединце и друштво у целини. Један од значајних циљева рада је и предлагање најбољих пракси и решења за превенцију оваквих инцидената. Поред тога, рад има за циљ да процени положај Републике Србије у односу на Европску унију када је реч о заштити података о личности, са посебним освртом на усклађеност са одредбама Опште уредбе о заштити података (ГДПР).

У раду ће бити примењени различити методолошки приступи, укључујући нормативну анализу правних аката, компаративну методу за поређење законодавстава

Европске уније и Републике Србије, као и студије случаја које ће послужити као примери за боље разумевање последица и ризика који се јављају у пракси. Такође ће се користити метода анализе садржаја релевантне литературе и судске праксе, посебно у контексту вештачке интелигенције и њеног утицаја на заштиту података, како би се додатно обогатило истраживање и допринело дубљем разумевању правног оквира који регулише ову област.

Структура рада је организована у више тематских целина. У првом делу се представља правни оквир заштите података о личности у Републици Србији. Други део рада бави се питањем повреде података, уз анализу узрока и околности које доводе до инцидената. У трећем делу разматрају се механизми превенције и управљања повредом података. У четвртом делу анализирају се последице повреде података, односно питања одговорности за повреде података о личности. Пети део истражује утицај вештачке интелигенције на обраду података, са посебним освртом на ризике и изазове који прате њену примену. Шести део рада посвећен је студијама случаја повреде података о личности у Републици Србији и Европској унији, док се у закључним разматрањима износе главни налази и предлози за унапређење постојећег система заштите.

II ПРАВНИ ОКВИР ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ И ЕВРОПСКОЈ УНИЈИ

Уставом Републике Србије, у члану 42, зајемчена је заштита података о личности. Став 2 овог члана прописује да се прикупљање, држање, обрада и коришћење података о личности уређују законом. Република Србија је 2018. године усвојила нови Закон о заштити података о личности, којим је његов истоимени претходник из 2008. године престао да важи. Овај, нови Закон о заштити података о личности, усвојен је под снажним утицајем европске Опште уредбе о заштити података (ГДПР)[1], али је добрим делом и адаптирани превод тзв. Полицијске директиве[2], која прописује правила за обраду података о личности коју врше надлежни органи у вези са кривичним поступцима и

[1] Уредба (ЕУ) 2016/679 Европског парламента и већа од 27. априла 2016. о заштити појединаца у вези са обрадом личних података и о слободном кретању таквих података те о стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података), *Службени лист ЕУ*, бр. L 119/1.

[2] Директива ЕУ 2016/680 Европског парламента и Већа о заштити појединаца у вези с обрадом података о личности од стране надлежних органа у сврхе спречавања, истраге, откривања или гоњења учинилаца кривичних дела или извршавања кривичних санкција и о слободном кретању таквих података, *Службени лист ЕУ*, бр. L 119/89.

претњама националној безбедности. У тренутку када је изгледало да је Србија, по угледу на Европску унију, добила један свеобухватан и ефикасан пропис који би служио као најважнији корак ка детаљној и сврсисходној регулацији ове изузетно важне области, убрзан развој технологије и система вештачке интелигенције довео нас је поново пред изазов и поставило се питање правног уређења заштите података о личности у условима широке употребе и развоја напредних модела вештачке интелигенције. Следом тога Република Србија је 2023. године усвојила Етичке смернице за развој, примену и употребу поуздане и одговорне вештачке интелигенције[3], а у јануару 2025. године и Стратегију развоја вештачке интелигенције за период 2025-2030. године[4]. Током 2024. године формирана је и радна група за израду Нацрта закона о вештачкој интелигенцији Републике Србије, а у изради закона, као пример, користи се између осталог и Акт о вештачкој интелигенцији Европске уније, познатији као AI Act, који детаљно регулише ову област.

Када говоримо о Европској унији, први значајан документ у овој области била је Конвенција 108 Савета Европе о заштити лица у односу на аутоматску обраду личних података која је ступила на снагу 1985. године, а заштита података о личности је први пут суштински регулисана 1995. године, Директивом ЕУ 95/46/ЕЗ Европског парламента и Савета о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података[5]. Овај пропис служио је првенствено као смерница за доношење националних закона у оквиру држава чланица. Ипак, управо овакав приступ довео је до неједнаког степена заштите у оквиру различитих држава, те се јавила потреба за усаглашавањем правила међу државама чланицама Европске уније. Усвајањем Повеље Европске уније о основним правима[6] из 2000. године, први пут у историји Европске уније, предвиђено је посебно право на заштиту података о личности. Првобитно само политички документ, стратешког значаја, ЕУ Повеља је постала правно обавезујућа у моменту кад је Лисабонски уговор ступио на снагу 1. децембра 2009[7]. До

[3] Закључак о усвајању етичких смерница за развој, примену и употребу поуздане и одговорне вештачке интелигенције, *Службени гласник РС,* бр. 23/2023.
[4] Стратегија развоја вештачке интелигенције у Републици Србији за период 2025-2030. године, *Службени гласник РС,* бр. 5/2025.
[5] Директива ЕУ 95/46/ЕЗ Европског парламента и Савета о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података, *Службени лист Еврпских заједница,* бр. L 281 од 23.11.1995. године.
[6] Повеља Европске Уније о основним правима, *Службени лист Европске уније,* бр. C 202 од 7.6.2016. године.
[7] Г. Гасми, *Quo vadis EU?- Релевантни правни и институционални фактори*, Београд, 2016, стр. 82.

доношења Повеље ЕУ о основним правима, право на заштиту података није експлицитно било издвајано као посебно фундаментално људско право на истом нивоу као и друга фундаментална људска права, већ се подразумевало да оно проистиче из права на приватност односно из права на поштовање приватног живота[8].

Захваљујући Повељи о основним правима ЕУ, отворен је простор за разговоре о усвајању прописа који ће на јединствен начин, на територији читаве ЕУ, регулисати питања од значаја у вези са заштитом података о личности. Након дуготрајне борбе грађана и невладиних организација, Европски парламент и Веће ЕУ предложили су доношење прописа који ће унификовати и оснажити заштиту свих лица у оквиру ЕУ. Као последица, усвојена је, можда и најзначајнија уредба у новијој историји ЕУ – Општа уредба о заштити података, 27. априла 2016. године, а своју примену је започела 25. маја 2018. године[9]. Ако је Општа уредба о заштити података (ГДПР) довела до прве револуције у регулисању ове области, може се рећи да је Акт о вештачкој интелигенцији (AI Act), који је усвојен 2024. године, изазвао другу револуцију, односно увео је правила којима се системи вештачке интелигенције класификују према степену ризика и поставио строге обавезе за оне системе који обрађују посебне категорије података о личности. У контексту заштите података, постоје подељени ставови у оквиру стручне јавности, у зависности од тога да ли се ради о стручњацима из технолошких наука или о правницима. Ови први сматрају да ће строга регулатива у овој области успорити развој и довести Европску унију (па и Републику Србију, уколико се угледа на ЕУ регулативу) у неповољан положај у односу на глобалне конкуренте, попут САД-а и Кине, јер постоји ризик да ће ригорозни правни оквир успорити технолошки развој, ограничити иновације и смањити конкурентност европских компанија на светском тржишту. Са друге стране, правници су углавном заузели став да је законско регулисање ове области апсолутно неопходно, те да би слободан приступ регулацији довео до озбиљних и несагледивих последица по права и слободе грађана.

[8] Г. Гасми, Д. Прља, Право на поштовање приватног живота и право на заштиту података о личности; у: Андоновић С., Прља Д., Дилигенски А. (ур.), *Заштита података о личности у Србији*, Београд, 2020, стр. 10.
[9] С. Андоновић, Д. Прља, *Основи права заштите података о личности*, Београд, 2020, стр. 120.

1. Закон о заштити података о личности Републике Србије

Република Србија је свој први пропис из области заштите података о личности имала још у оквиру правног система Савезне Републике Југославије. Био је то Закон о заштити података о личности из 1998. године[10], а који је усвојен у циљу испуњења обавеза које је СРЈ имала као потписница Конвенције Савета Европе бр. 108 о заштити лица у погледу аутоматске обраде података о личности[11]. Ипак, овај закон, иако је био усклађен са Конвенцијом 108, није био усклађен са Директивом ЕУ 95/46/ЕЗ Европског парламента и Савета о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података, те је са становишта европских прописа, као такав, био превазиђен. Наиме, закон није регулисао прикупљање, обраду и коришћење података о личности, јер је то требало да буде регулисано посебним законима, који никада нису донети. Република Србија, као правни следбеник некадашње СРЈ, а касније и државне заједнице СЦГ, је приликом преношења надлежности са савезних органа на органе Републике Србије, дошла у ситуацију да није био одређен државни орган који би преузео надлежност за остваривање права по овом закону, те је самим тим изостала и практична примена овог закона.

Током процеса европских интеграција, Србија је у октобру 2008. године закључила Споразум о стабилизацији и придруживању са Европском унијом, и поднела захтев за чланство у ЕУ у децембру 2009. године. Овај Споразум, између осталог, садржи и обавезу Србије да хармонизује своје законодавство о заштити података о личности са правом ЕУ и другим релевантним европским и међународним стандардима (чл. 8)[12]. Следом наведеног, у октобру 2008. године уследило је доношење новог Закона о заштити података о личности[13], а који је ступио на снагу јануара 2009. године. Овим законом уређени су услови за прикупљање и обраду података о личности, као и права лица чији се подаци прикупљају и обрађују. Међутим, најважнија иновација овог закона било је

[10] Закон о заштити података о личности, *Службени лист СРЈ*, бр. 24/98 и 26/98 - исправка.
[11] Конвенција Савета Европе о заштити лица у односу на аутоматску обраду личних података (Конвенција 108) је потврђена усвајањем Закона о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података, *Службени лист СРЈ - Међународни уговори, бр. 1/92, Службени лист СЦГ – Међународни уговори, бр. 11/2005 - др. закон и Службени гласник РС - Међународни уговори, бр. 98/2008 - др. закон и 12/2010.*
[12] С. Лилић, Инспекцијска и друга овлашћења Повереника за заштиту података о личности; у: Андоновић С., Прља Д., Дилигенски А. (ур.), *Заштита података о личности у Србији*, Београд, 2020, стр. 107-108.
[13] Закон о заштити података о личности*, Службени гласник РС*, бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012.

успостављање посебног органа за заштиту података о личности у Србији, односно Повереника за информације од јавног значаја и заштиту података о личности.

Под утицајем доношења Опште уредбе ЕУ, Република Србија је у новембру 2018. године усвојила нови Закон о заштити података о личности, чији основни циљ је био усклађивање са Општом уредбом ЕУ, али и Полицијском директивом. На овај начин су основна начела и правила Опште уредбе ЕУ и Полицијске директиве уведени на домаћи терен. Ипак, већ након усвајања, а и касније током примене закона, уочени су значајни недостаци овог прописа. Пре свега, законодавац је пропустио да нормативно разради нека од кључних начела, института и појмова који су у Општој уредби ЕУ образложени у преамбули, па је тако српски закон остао нејасан и без објашњења појединих института који су њиме по први пут уведени у наш правни систем. Поред тога, нови закон је прописао знатно блаже санкције у односу на оне које су прописане Општом уредбом ЕУ, а у пракси се показало да постоје бројна нерешена питања и у вези са начином примене прописаних санкција. Неспретан превод појединих термина са енглеског језика, као што је превод термина ”*establishment*” као ”седиште”, довео је до нелогичности и проблема у примени прописа. Формулација члана 3 став 3 Закона о заштити података о личности резултирала је суженом територијалном применом српског закона у односу на територијалну примену Опште уредбе ЕУ. Ова одредба прописује да се закон примењује на обраду података о личности коју врши руковалац, односно обрађивач који има седиште, односно пребивалиште или боравиште на територији Републике Србије, у оквиру активности које се врше на територији Републике Србије, без обзира да ли се радња обраде врши на територији Републике Србије. Насупрот томе, члан 3 став 1 Опште уредбе ЕУ предвиђа да се уредба примењује на обраду у контексту активности *establishment*-а руковаоца или обрађивача у ЕУ. Суд правде ЕУ и Европски одбор за заштиту података о личности су појаснили да *establishment* постоји и када један или више представника привредног друштва регистрованог ван ЕУ делује са ”довољним степеном стабилности” кроз присуство у ЕУ[14][15]. Тачка 22 преамбуле Опште уредбе ЕУ прецизира да се седиштем сматра свако ефикасно и стварно обављање делатности кроз стабилне аранжмане, при чему правни облик таквих аранжмана није одлучујући фактор у том погледу. Насупрот томе, према нашем закону, територијална примена зависи од тога да

[14] Case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, para. 30
[15] European Data Protection Board. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1*, Brussels, 2019, p. 6-7.

ли руковалац или обрађивач има седиште у Србији, што подразумева место и адресу из које се управља пословањем друштва и које је као такво одређено оснивачким актом, статутом или одлуком скупштине, односно ортака или комплементара[16]. Руковалац и обрађивач у српском закону дефинисани су као „физичко или правно лице, односно орган власти“. Имајући у виду да огранци и представништва страних правних лица, у складу са Законом о привредним друштвима, немају својство правног лица, већ представљају издвојени организациони део страних правних лица[17], долазимо до ситуације у којој они формално остају изван примене Закона о заштити података о личности, иако послују на територији Републике Србије. Широко је распрострањено мишљење да би се овај проблем могао решити увођењем термина ”пословни настан” у српско законодавство, а који би обухватио и оне ентитете који не могу бити обухваћени појмом ”седиште”. Такође, постоје ставови да је неопходно посебно уредити положај огранака и представништва страних правних лица, како би се отклониле недоумице у вези примене закона на њих.

Почетком марта 2025. године, Влада Републике Србије усвојила је Акциони план за спровођење Стратегије заштите података о личности за период до 2030. године, а као посебно истакнута мера чије ће спровођење бити омогућено овим Акционим планом, јесте измена и допуна постојећег Закона о заштити података о личности, или пак, доношење новог закона.

2. Општа уредба ЕУ о заштити података о личности

Уредбе у правном систему Европске уније имају посебан значај јер се директно примењују у свим њеним чланицама, без потребе за усвајањем на нивоу појединачних држава. Оне доприносе правној сигурности и уједначености у примени закона унутар ЕУ, а што омогућава несметано функционисање јединственог тржишта и заштиту права грађана. Једнака правна снага уредби у свим државама чланицама обезбеђује висок степен правне усклађености националних законодавстава.

[16] Чл. 19 Закона о привредним друштвима, *Службени гласник РС*, бр. 6/2011, 99/2011, 83/2014 - др. закон, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021 и 19/2025.
[17] Члан 567 став 2 и члан 574 став 2 Закона о привредним друштвима, *Службени гласник РС*, бр. 6/2011, 99/2011, 83/2014 - др. закон, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021 и 19/2025.

Општа уредба ЕУ успоставила је највише стандарде заштите података о личности и представља најсвеобухватнији правни оквир у историји. Четири године је трајало усаглашавање коначне верзије текста ове уредбе (2012-2016), а у јавној расправи учествовали су бројни субјекти из јавног и приватног сектора. Број амандмана од чак 4000, указује на огромно интересовање које је ова уредба изазвала у ЕУ.

Значај ове уредбе огледа се у томе што поставља строге стандарде за све руковаоце и обрађиваче са седиштем у ЕУ, независно од тога да ли се обрада обавља на територији ЕУ или ван ње (територијално важење), али и за руковаоце и обрађиваче који немају седиште у ЕУ, уколико су њихове активности повезане са понудом робе или услуга лицима у ЕУ или праћењем понашања лица у ЕУ, докле год се њихова делатност одвија у ЕУ (екстериторијално важење). Једно од најважнијих начела Опште уредбе ЕУ јесте начело транспарентности и контроле, а које појединцима даје право да знају како се њихови подаци користе, да им приступе, па чак и да траже њихово брисање ако за то постоји основ. Овај механизам је постао познат као ”право на заборав”, а омогућио је грађанима већу контролу над својим дигиталним трагом. Општа уредба такође поставља обавезу руковаоцима и обрађивачима да обезбеде изричит, информисан и јасан пристанак лица чији подаци се обрађују, пре саме обраде таквих података. Поред тога, организације које предузимају радње обраде дужне су да у случају повреде података обавесте надлежне органе, али и лица на које се подаци односе, у року од 72 сата, чиме се уводи нови ниво одговорности. Велики значај има и право на преносивост података, које омогућава лицима на које се подаци односе да своје податке лако пренесу са једног руковаоца на другог. Субјекти који обрађују велике количине података, у складу са уредбом, обавезни су да именују лице за заштиту података, које је задужено за надгледање усаглашености са регулативом. На крају, али можда и најважнији механизам уредбе, јесу астрономске казне за непоштовање прописа, које могу износити и до 20 милиона евра или 4% годишњег глобалног прихода компаније. Овај механизам је осигурао да организације широм света озбиљно приступе заштити података, чинећи Општу уредбу ЕУ једним од најстрожих и најефикаснијих прописа у дигиталном добу.

3. Полицијска директива

Директиве у правном систему Европске уније имају кључну улогу у усклађивању законодавстава држава чланица. Оне постављају циљеве које земље морају постићи, али

им остављају слободу у избору начина увођења у национална законодавства. За разлику од уредби, које се директно примењују у свим државама чланицама без потребе за додатним усвајањем, директиве захтевају да се њихове одредбе унесу у националне законе. Овај механизам омогућава флексибилност у примени прописа, прилагођавајући их специфичностима сваке државе, док истовремено осигурава правну хармонизацију унутар ЕУ.

Директива ЕУ 2016/80, познатија као Полицијска директива, представља важан правни оквир за заштиту података о личности у вези са њиховом обрадом од стране надлежних органа, а у циљу спречавања, истраге, откривања или гоњења учинилаца кривичних дела или извршења кривичних санкција, као и за омогућавање слободног кретања таквих података. Усвојена је 2016. године као део пакета реформи у области заштите података, а примењује се од 2018. године, заједно са Општом уредбом ЕУ.

У односу на Општу уредбу ЕУ, Полицијска директива у појединим аспектима садржи мање строге стандарде, али у неким другим аспектима она уводи прилагођена решења за потребе полицијских и правосудних органа. Наиме, за разлику од Опште уредбе ЕУ, Полицијска директива не захтева исти ниво транспарентности у обради података, што омогућава надлежним органима већу флексибилност у раду. Осим тога, начело минимизације обраде је ублажено, што значи да полицијски органи могу обрађивати шири обим података уколико оперативне потребе то захтевају. Такође, права појединаца на заштиту података могу бити значајно ограничена ако би њихова примена угрозила истрагу или националну безбедност. Полицијском директивом су само оквирно дефинисана овлашћења надлежних надзорних тела у државама чланицама, док Општа уредба ЕУ детаљно прописује њихову улогу и обавезе.

Са друге стране, Полицијска директива садржи и одредбе које су специфичне за област њеног деловања и које не постоје у Општој уредби ЕУ. Једна од њих је и обавеза категоризације лица и њихових података, што омогућава ефикасније управљање подацима у полицијским евиденцијама. Директива такође предвиђа и обавезу утврђивања рокова за чување података о личности, што спречава њихову неограничену обраду и чување. Поред тога, прописано је вођење детаљне евиденције о сваком приступу подацима и свакој обради података, чиме се осигурава одговорност у руковању изузетно осетљивим подацима.

Дакле, Полицијска директива настоји да пронађе равнотежу између потребе за ефикасним кривичним гоњењем и обезбеђењем јавне безбедности и сигурности свих грађана, са једне стране, и заштите података о личности грађана као једног од основних права, са друге стране. Она то постиже тако што истовремено обезбеђује одређену дозу флексибилности надлежним органима, али и гарантује контролу и одговорност приликом обраде података грађана од стране тих органа.

4. Акт о вештачкој интелигенцији Европске уније

Појава ChatGPT-а и сличних система заснованих на технологијама вештачке интелигенције и њихова популарност коју су стекли током 2023. године, поново је ставила европског законодавца пред изазов када је у питању заштита основних права грађана, а посебно заштита приватности и података о личности. Након што је компанија OpenAI током 2022. године лансирала верзију GPT-3.5 свог чет-бота заснованог на великом језичком моделу, ова услуга је постала широко популарна, а процењено је да је стекла око 100 милиона активних корисника већ до јануара 2023. године. Ова дешавања приморала су законодавне органе ЕУ да што пре усвоје регулаторни оквир који би уредио развој и употребу вештачке интелигенције, што је резултирало усвајањем тзв. Акта о вештачкој интелигенцији, 21. маја 2024. године[18].

Након скоро три године интензивног рада и сложених преговора, законодавци Европске уније постигли су договор о Акту о вештачкој интелигенцији, који дефинише регулаторни оквир за технологије вештачке интелигенције које се користе широм ЕУ. Суштина ове регулативе је промоција развоја технологија вештачке интелигенције усмерених на људе и заснованих на поверењу, уз очување основних права и темељних вредности ЕУ[19]. Међутим, иако усвајање овог акта представља значајан корак напред, његови амбициозни циљеви не могу се постићи самим доношењем прописа. Уместо тога, он покреће следећу фазу политичког циклуса, која укључује успостављање институционалних структура, доношење извршних аката, хармонизованих стандарда,

[18] Уредба (ЕУ) 2024/1689 Европског парламента и Савета од 13. јуна 2024. о утврђивању усклађених правила о вештачкој интелигенцији и мењању Уредбе (ЕЗ) бр. 300/2008, (ЕУ) бр. 167/2013, (ЕУ) бр. 168/2013, (ЕУ) 2018/858, (ЕУ) 2018/1139 и (ЕУ) 2019/2144, као и Директиве 2014/90/ЕУ, (ЕУ) 2016/797 и (ЕУ) 2020/1828 (Акт о вештачкој интелигенцији), *Службени лист Европске уније,* бр. L 1689 од 12.7.2024. године.
[19] *ibid.,* члан 1.

смерница и кодекса праксе, а затим њихову интерпретацију и имплементацију од стране свих циљних актера[20].

Европски Акт о вештачкој интелигенцији заправо је први свеобухватни законски оквир у свету, који систематски регулише развој, употребу и надзор над системима вештачке интелигенције. Као једну од основних новина, ова уредба увела је тзв. ”приступ заснован на ризику”. Дакле, Акт о вештачкој интелигенцији класификује системе вештачке интелигенције у различите категорије зависности од нивоа ризика који такви системи представљају за основна права грађана, али и за националну безбедност и демократско друштво. Прва категорија обухвата потпуно забрањене употребе, као што су системи који користе подсвесне технике ради утицаја на људско понашање, системи за социјално оцењивање грађана, неовлашћено прикупљање слика лица путем интернета и видео-надзора, предиктивно полицијско поступање усмерено ка појединцима, као и даљинска биометријска идентификација у реалном времену за потребе спровођења закона – осим у строго ограниченим околностима (члан 5 AI Act). Друга категорија обухвата системе високог ризика, за које се прописује посебан режим усклађености. Ови системи обухватају, с једне стране, технологије вештачке интелигенције које су део хармонизованих производа у оквиру Новог законодавног оквира ЕУ (Анекс II), а с друге стране, системе наведене у Анексу III, који се односе на примене које могу имати значајан утицај на људска права или животну средину, као што су биометрија, критична инфраструктура, образовање, запошљавање, полицијско поступање, правосуђе и демократски процеси. Многе од ових примена присутне су у јавном сектору, што додатно наглашава потребу за прецизном и одговорном применом прописа. Трећа категорија обухвата примене које носе ограничен ризик, као што су чет-ботови, „дипфејк“ технологије и системи за препознавање емоција. За ове примене довољно је да корисници буду обавештени да комуницирају са системом вештачке интелигенције (члан 50 AI Act). Четврта категорија односи се на системе вештачке интелигенције опште намене (GPAI), укључујући велике језичке моделе и друге основне моделе вештачке интелигенције. Ови системи посебно су регулисани у завршној фази усвајања Акта о вештачкој интелигенцији, имајући у виду њихов потенцијал да системски утичу на друштво. За оне моделе који имају висок капацитет утицаја, процењен техничким алатима или одлуком Европске комисије, предвиђен је посебно строг режим

[20] K. Söderlund, S. Larsson, Enforcement Design Patterns in EU Law: An Analysis of the AI Act, *Digital Society*, no. 41, Vol. 3, pp. 2.

усклађености (члан 51 AI Act). Најзад, све преостале примене које нису забрањене, те не спадају у високо ризичне, нити у категорију система вештачке интелигенције опште намене (GPAI), сврстане су у најнижи ризични ниво. За ову категорију не постоје значајне обавезе, осим примене добровољних кодекса понашања (члан 95 AI Act)[21].

Поред тога, овај пропис захтева транспарентност, обавезује добављаче и кориснике високоризичних система вештачке интелигенције да обезбеде адекватне мере заштите, те забрањује одређене праксе као што су манипулативни системи вештачке интелигенције и биометријски надзор у реалном времену на јавним просторима. Такође, овај пропис уводи централизовани механизам надзора на нивоу ЕУ, уз координацију националних тела за спровођење и контролу примене ових правила. На овај начин, Акт о вештачкој интелигенцији не само да поставља чврсте темеље за правну сигурност у области вештачке интелигенције, већ позиционира Европску унију као глобалног лидера у регулацији технологија заснованих на вештачкој интелигенцији.

III ПОВРЕДА ПОДАТАКА: АНАЛИЗА УЗРОКА И ОКОЛНОСТИ КОЈЕ ДОВОДЕ ДО ИНЦИДЕНАТА

1. Повреда података о личности

”Ми знамо где се налазите. Ми знамо где сте били. Ми, мање-више, знамо о чему размишљате.[22]” Овим речима је у октобру 2010. године тадашњи извршни директор компаније Гугл, током другог годишњег форума Washington Ideas, илустровао домет савремених технологија у прикупљању и обради података. Данас, сведочимо ери у којој се лични подаци корисника многобројних услуга у онлајн окружењу користе у несагледивом обиму, док се питање приватности поставља као један од најизазовнијих аспеката дигиталног доба. Степен надзора и обраде података о личности достигао је историјски максимум, а то отвара бројна етичка, правна и друштвена питања у погледу заштите приватности и безбедности података.

У једној студији коју је IBM спровео 2015. године процењено је да просечан трошак повреде података износи око 3,8 милиона америчких долара по инциденту. Повреда

[21] *ibid.,* pp. 9-10.
[22] D. Thompson, *Google's CEO: 'The Laws Are Written by Lobbyists'*, (2010); преузето 3.4.2025. https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/

података у телекомуникационој компанији TalkTalk 2015. године процењена је на 35 милиона фунти. Један инцидент повреде података у америчком ланцу малопродаје Target процењен је на 162 милиона долара, уз пад продаје од 5,3%. Повреде података могу такође представљати радњу извршења кривичног дела за коју се лица могу кривично гонити. Поред тога, лична одговорност може се приписати запосленима у организацији, и то као одвојена, али и као додатна одговорност поред одговорности саме организације[23].

Податак о личности је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета[24]. Дакле, да би се неки податак сматрао податком о личности у складу са законом, он мора да се односи на неко одређено или одредиво физичко лице. Ова дефиниција не обухвата податке о правним лицима. Такође, ова законска дефиниција односи се само на податке живих физичких лица. Тачком 27 преамбуле Опште уредбе о заштити података ЕУ прописано је да се ова уредба не примењује на податке преминулих лица, али како је српски законодавац пропустио да у наше законодавство унесе одредбе преамбуле Опште уредбе, ово питање је остало недоречено.

Уколико посматрамо онлајн окружење, међу податке о личности спадају нарочито и идентификатори интернет мреже (IP адресе – динамичке и статичке), колачићи које користе уређаји и сајтови, MAC адресе уређаја, идентификације са базних станица (Cell-ID), подаци са WI-FI рутера, апликације, подаци са дебитних и кредитних картица, биометријски подаци (отисак прста, препознавање лица, дужице ока, облика ушију, препознавање гласа, идентификација потписа, анализа куцања по тастатури, анализа хода, и слично), фотографије направљене биометријским технологијама, али и слике које показују нашу верску припадност.

Подаци о личности представљају можда и најзначајнију категорију података у области права, будући да се њима штити приватност грађана. Због огромног значаја,

[23] P. Lambert, *The Data Protection Officer: Profession, Rules, and Role*, Boca Raton, 2017, pp. 7.
[24] Члан 4 став 1 тачка 1 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/18.

приватности у савременом друштву и подаци о личности уживају посебну заштиту, будући да њиховом повредом може доћи и до повреде интегритета и приватности физичких лица. Они се односе на одређени психички, физички, социјални или други јединствени и непоновљиви елемент личности[25].

Повреда података о личности је повреда безбедности података о личности која доводи до случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања или приступа подацима о личности који су пренесени, похрањени или на други начин обрађивани[26]. Дакле, када говоримо о повреди података заправо говоримо о три основна аспекта повреде података: повреди поверљивости, интегритета и доступности података. Ова три аспекта повреде података могу најбоље да се објасне кроз модел информационе безбедности осмишљен за заштиту посебно осетљивих података, тзв. CIA тријада (confidentiality, integrity, availability).

Поверљивост се односи на предузимање мера ради контроле приступа подацима и осигурање да подаци буду доступни само овлашћеним особама, односно предузимање свих неопходних активности да се спречи неовлашћен приступ подацима о личности. Такође, Законом о заштити података о личности је установљено начело интегритета и поверљивости, па је прописано да се подаци о личности морају обрађивати на начин који обезбеђује одговарајућу заштиту података о личности, укључујући заштиту од неовлашћене или незаконите обраде, као и од случајног губитка, уништења или оштећења применом одговарајућих техничких, организационих и кадровских мера[27]. Повреда поверљивости података најчешће се дешава услед неовлашћеног приступа или злоупотребе осетљивих информација. Један од можда најзначајнијих примера повреде поверљивости података догодио се у случају Едварда Сноудена, бившег службеника Националне безбедносне агенције САД-а, који је 2013. године обелоданио поверљиве документе о програмима масовног надзора. Овај случај је покренуо глобалну дебату о приватности и етици у обавештајним службама[28].

[25] З. Јовановић, С. Андоновић, Врсте информација и података у јавном праву Републике Србије; у: Андоновић С., Прља Д., Дилигенски А. (ур.), *Заштита података о личности у Србији*, Београд, 2020, стр. 37.
[26] Члан 4 став 1 тачка 13 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/18.
[27] Члан 5 став 1 тачка 6 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/18.
[28] A. Carlson, *Edward Snowden: Traitor or Hero*, (2022); преузето 3.4.2025. https://ethicsunwrapped.utexas.edu/case-study/edward-snowden-traitor-hero

Интегритет података односи се на обавезу руковаоца и/или обрађивача да обезбеде да подаци остану тачни, комплетни и непромењени, односно да се спрече њихове измене, брисања или додавања без одобрења. Један од најозбиљнијих облика угрожавања интегритета података у дигитално доба су тзв. рансомвер напади, у којима злонамерни софтвер шифрује податке жртве и онемогућава њихов приступ, уз захтев за откупнину како би се повратила контрола над њима. Откупнина се по правилу тражи и исплаћује у криптовалутама, најчешће у биткоину. Трансакцијама у криптовалутама је тешко пратити траг, те је њихово коришћење у функцији очувања анонимности нападача[29]. Овакви напади неретко доводе до нарушавања интегритета података јер корисник, након поновног успостављања контроле над подацима, више не може да гарантује да су подаци аутентични и непромењени. Напади овог типа, уколико циљају на ИКТ системе од посебног значаја, представљају озбиљан изазов не само за национално законодавство већ и за доносиоце политичких одлука и креаторе националних безбедносних политика. ИКТ системи од посебног значаја су системи који се користе у обављању послова у органима јавне власти, за обраду података о личности и у обављању делатности од општег интереса (члан 6, Закон о информационој безбедности, „Службени гласник РС“, 6/2016 и 94/2017). Ови системи се у англосаксонском говорном подручју уобичајено називају критичном информационом инфраструктуром која представља једну од посебно осетљивих критичних инфраструктура државе[30]. Један од најпознатијих примера рансомвер напада је напад WannaCry из 2017. године, који је погодио више од 200 000 система у преко 150 земаља, укључујући и болнице, банке и државне институције[31]. Осим финансијске штете, овакви напади могу довести и до критичних последица, као што је угрожавање људских живота.

Доступност се односи на осигурање да подаци буду доступни за употребу када су потребни овлашћеним корисницима. Ово подразумева предузимање мера и одржавање система који ће обезбедити континуиран приступ подацима, као и адекватно реаговање у случају инцидента који може на било који начин угрозити приступ (нпр. у болници, ако подаци о пацијентима нису доступни, чак и привремено, операције могу бити отказане, а пацијенти угрожени). У савремено доба, један од најчешћих напада на

[29] Н. Путник, М. Милошевић, В. Цветковић, Рансомвер као претња безбедности – друштвени и кривичноправни аспекти, *Социолошки преглед,* бр. 1, Vol. 56*,* стр. 329.
[30] *ibid.,* стр. 329.
[31] N. Sharma, *Case Study: The WannaCry Ransomware Attack*, (2024); преузето 3.4.2025. https://medium.com/@nitishsharma9136/case-study-the-wannacry-ransomware-attack-c010789be119

доступност података јесу тзв. напади ускраћивања услуге (DDoS – Distributed Denial of Service), који функционишу тако што нападачи шаљу огроман број захтева серверима, што доводи до њиховог преоптерећења и онемогућавања приступа легитимним корисницима. Овакви напади не морају нужно да доведу до крађе података, али могу имати значајне последице, поготово ако су усмерени на критичну инфраструктуру. Један од највећих оваквих напада забележен је 2016. године када је нападнут провајдер Dyn, што је довело до привременог обарања сервиса као што су Twitter, Netflix, PayPal и Reddit[32].

Све већа зависност од дигиталних технологија и глобална умреженост довеле су до околности у којима се подаци о личности грађана налазе у континуираном ризику од разних злоупотреба, било кроз циљане сајбер нападе, било кроз системске пропусте или људске грешке. Као што је и приказано, повреда поверљивости, интегритета и доступности података може имати далекосежне последице, од финансијских губитака, па до нарушавања основних права и слобода грађана. Разумевање ових аспеката је од кључног значаја за успостављање адекватних безбедносних мера и правног оквира који би умањио ризике.

2. Пракса Повереника за информације од јавног значаја и заштиту података о личности у Републици Србији

Повереник за информације од јавног значаја и заштиту података о личности је у свом, јубиларном, 20. годишњем извештају о раду навео да је у 2024. години у области заштите података о личности Служба Повереника обавила рекордан број инспекцијских надзора над обрадом података о личности од стране руковалаца из разних области живота [33].

Повереник је посебно нагласио да је током 2024. године безбедност података о личности била знатно угрожена, посебно успостављањем нових информационих система путем којих се обрађује велики број осетљивих података о грађанима, а када је у питању

[32] S. Thielman, C. Johnston, *Major cyber attack disrupts internet service across Europe and US*, (2016); преузето 3.4.2025. https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service
[33] Повереник за информације од јавног значаја и заштиту података о личности. *Извештај о раду за 2024. годину*, Београд, 2025, стр. 6.

структура руковалаца над којима је Повереник покренуо поступак инспекцијског надзора, наводи се да је највећи број таквих поступака вршен над јавним предузећима[34].

Како се из Извештаја види, током 2024. године у Републици Србији је изјављен рекордан број притужби Поверенику (њих 228) у односу на све претходне године од почетка примене новог Закона о заштити података о личности. Најчешћи разлог за подношење притужбе Поверенику био је одбијање захтева за остваривање права од стране руковаоца (129 притужби), а онда и због тога што руковаоци нису поступали по захтеву за остваривање права у законом прописаном року од 30 дана (51 притужба), али и због тога што су само делимично поступали по захтеву (47 притужби)[35].

Захтеви поводом којих су, због одговарајућег непоступања руковалаца, подношене притужбе Поверенику, односе се на остваривање права: на приступ подацима (66,1%), на брисање података о личности (32,2%), на исправку и допуну (1,3%) и прекид обраде (0,4%)[36].

Сумирајући наведене податке, може се закључити да је током 2024. године у Републици Србији дошло до значајног интензивирања активности у области заштите података о личности, како са становишта надзорних органа, тако и у погледу ангажовања грађана у остваривању својих права. Рекордан број извршених инспекцијских надзора и притужби упућених Поверенику, указују на растућу свест јавности о значају заштите података, али исто тако и на постојеће системске недостатке у поступању руковалаца. Учестале повреде права, посебно права на приступ, брисање и исправку података, као и честа непоступања у законом прописаним роковима, сведоче о потреби даљег јачања капацитета како контролних тела, тако и самих руковалаца. Наведено стање недвосмислено указује на то да се у наредном периоду морају уложити додатни напори у правцу унапређења праксе примене закона и подизања нивоа безбедности грађана при обради њихових података, нарочито у раду јавног сектора.

[34] *ibid*., стр. 106.
[35] *ibid.,* стр. 115.
[36] *ibid.,* стр. 19.

3. Узроци и околности који доводе до инцидената

Анализом доступне праксе, како на националном, тако и на међународном нивоу, може се закључити да се инциденти у области заштите података о личности најчешће јављају као резултат комбинације више фактора. Кључни узроци и околности који доводе до повреда података о личности могу бити сагледани кроз три основне категорије: техничке узроке, утицај људског фактора и правне, односно организационе недостатке. Ова подела омогућава систематичан приступ анализи инцидената и пружа основу за разумевање комплексности овог проблема, као и за формулисање адекватних мера за њихову превенцију и спречавање.

3.1. Технички узроци

Тренд коришћења интернета и уопште модерних технологија обухватио је све области живота. Са друге стране убрзани развој технологије довео је до могућности комерцијализације података о личности. До комерцијализације података може доћи злоупотребом технологије (нпр. коришћењем видео надзора, алата вештачке интелигенције, итд.) као и свесном продајом података о личности од стране појединаца, држава, компанија, професионалних продаваца података о личности. Појединци нису свесни могућности злоупотреба и ризика у вези са комерцијализацијом података о личности. Са напретком технологије овај недостатак је све већи, пошто техничке могућности постају све веће, комплексније и софистицираније[37].

Технички узроци који доводе до повреда података о личности су значајан фактор у настанку инцидената у области информационе безбедности. Најчешћи технички пропусти огледају се у недовољној заштити система од сајбер напада, у коришћењу застарелих софтвера, као и у недостатку примене напредних метода шифровања података. Овакви пропусти доводе до повећаног ризика од неовлашћеног приступа, крађе, измене или уништења података.

[37] А. Дилигенски, Вредност података о личности; у: Андоновић С., Прља Д., Дилигенски А. (ур.), *Заштита података о личности у Србији*, Београд, 2020, стр. 19.

Масовна употреба друштвених мрежа представља један од најзначајнијих техничких узрока који доприносе повредама података о личности у савременом дигиталном окружењу. Велики обим обраде података о личности, недовољно транспарентне и преобимне политике приватности, као и комплексност техничких система који стоје иза оваквих платформи повећавају ризик од инцидената. Значајан пример техничких пропуста може се уочити кроз анализу случаја Фејсбука. У пракси се показало да су нпр. фотографије које су корисници обрисали са својих профила остале доступне преко директних линкова месецима након њиховог брисања, што указује на озбиљне недостатке у процедурама управљања подацима и архитектури система. Сваки корисник Фејсбука који познаје УРЛ адресу одређене слике, може јој приступити и након њеног брисања. То је могуће учинити и након 16 месеци од брисања слике уношењем УРЛ адресе. Неки корисници су оваквим поступком дошли и до фотографија, које су званично биле обрисане пре три године[38]. Поред тога, Фејсбук је користио колачиће за праћење активности корисника чак и када нису били пријављени на платформу, чиме је значајно повећан ризик од неконтролисаног прикупљања и обраде података о личности. Фејсбук уз помоћ свог дата-колачића (енг. Cookie) неовлашћено прати понашање корисника везано за њихово сурфовање по интернету. Фејсбук је информисао кориснике само о томе да је овај колачић у употреби да би се прикупиле информације са спољних платформи. Корисници Фејсбука нису информисани о томе, по мишљењу Националне француске комисија за информатику и слободе, да Фејсбук том приликом сваки пут прикупља информације о њима када посете неки веб сајт, који садржи друштвене додатке „social-plugin“. Осим тога овим колачићем се прикупљају и подаци осталих интернет корисника, који нису корисници Фејсбука, када посећују веб сајтове који садржи друштвене додатке „social-plugin“[39].

Ови примери показују да пропусти у дизајну, имплементацији и надзору техничких система значајно доприносе повредама података о личности, те да је неопходно успостављање строгих безбедносних мера од самог почетка пројектовања информационих система (*privacy by design* приступ).

[38] А. Дилигенски, Д. Прља, *Фејсбук, заштита података и судска пракса*, Београд, 2018, стр. 24.
[39] *ibid.,* стр. 95.

3.2. Људски фактор

Људски фактор представља један од најзначајнијих узрока због којих долази до повреде података о личности. И поред примене најсавременијих техничких мера заштите, људске грешке, немар, као и недовољна свест о значају заштите података, често воде ка озбиљним пропустима и инцидентима.

Најчешће се ризици који потичу од људског фактора односе на непоштовање интерних безбедносних политика, на неправилно руковање посебним категоријама података о личности, слабу контролу приступа подацима, нехатно откривање поверљивих података путем електронске поште или друштвених мрежа, неразумевање потребе за коришћењем сложених лозинки, недовољна информатичка писменост, и слично. Недовољно обучени или неодговорни запослени могу представљати ”најслабију карику” у систему заштите података. Поред ненамерних грешака, све чешће се јављају и намерне злоупотребе података од стране запослених, посебно у оквиру организација које нису адекватно регулисале приступ, обраду и коришћење података о личности и уопштено поверљивих података.

У овом тренутку, свест појединаца о заштити приватности је недовољна; навикнути су да се ослањају на интернет услуге и немају адекватно разумевање концепта приватности, нити свест о ризицима. Иако појединци тврде да придају велики значај заштити приватности, њихово стварно понашање често демантује ту тврдњу. Научници овај јаз између декларисаних ставова о приватности и стварног понашања у пракси дефинишу као ”парадокс приватности”[40]. „Парадокс приватности“ указује на то да млади људи тврде да им је стало до приватности, док истовремено објављују велику количину личних података на друштвеним мрежама[41].

Пракса показује да су континуирана едукација грађана, увођење обавезних обука запослених о заштити података и унапређење културе безбедности у оквиру самих организација, кључне мере у смањењу ризика од повреда које произлазе из људског фактора.

[40] M. Wang, Y. Qin, J. Liu, W. Li, Identifying personal physiological data risks to the Internet of Everything: the case of facial data breach risks, *Humanities and Social Sciences Communications*, no. 216, Vol. 10, pp. 10.
[41] E. Hargittai, A. Marwick, “What Can I Really Do?” Explaining the Privacy Paradox with Online Apathy, *International Journal of Communication,* Vol. 10, pp. 3737.

3.3. Правни и организациони недостаци

Правни и организациони недостаци значајно утичу на настанак, али и на тежину повреда података о личности. У многим случајевима, повреде се дешавају због непотпуне или неадекватне примене законских прописа, а неретко и због потпуног изостанка примене истих. Такође, велики број повреда настаје и због неуспостављених или недовољно јасних интерних политика и процедура у оквиру организација које обрађују податке о личности.

Најчешћи правни пропусти огледају се у непоштовању начела законитости, поштења и транспарентности обраде података о личности[42] кроз ускраћивање информација које је руковалац дужан да пружи лицу на које се подаци односе, обраду података супротно сврси за коју су прикупљени[43], повреди начела минимизације обраде података[44], непостојању уговора о обради података са обрађивачима[45], као и у пропустима у правовременом обавештавању надзорних тела[46] и лица на која се подаци односе[47] у случају повреде.

Организациони недостаци, као што су недостатак јасно дефинисаних улога и одговорности у процесу заштите података у оквиру организације, одсуство службеника за заштиту података у ситуацијама када је његово ангажовање законом прописано и у пракси неопходно, као и несистематичан приступ процени ризика, додатно повећавају изложеност повредама. Савремени стандарди добре праксе налажу да организације успоставе свеобухватне програме управљања заштитом података, укључујући редовну процену усклађености са прописима, увођење принципа уграђене приватности и подразумеване приватности (енг. *Privacy by design, Privacy by default*), као и спровођење редовних контрола како би се благовремено уочиле слабости и предузеле корективне мере.

Велику пажњу у стручној јавности привукла су два принципа која Општа уредба ЕУ установљава у вези са обавезама руковаоца. То су принцип подразумеване приватности

[42] Чл. 5 став 1 тачка 1 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[43] Чл. 5 став 1 тачка 2 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[44] Чл. 5,став 1 тачка 3 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[45] Чл. 45 став 3 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[46] Чл. 52 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[47] Чл. 53 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

(*Privacy by default*) и принцип уграђене приватности (*Privacy by design*). Ови принципи уско су повезани са новим тржиштима, дигиталном економијом и индустријом 4.0. На тај начин развој технологије и технике препознат је и у правним оквирима. Принцип подразумеване приватности односи се на проактивни приступ у вези са заштитом података о личности, још од првих фаза развијања поједине услуге или добра. Дакле, у циљу поштовања овог принципа потребно је водити рачуна о мерама заштите и безбедности података о личности, већ приликом планирања средстава и начина обраде, што подразумева и њихову имплементацију током процеса обраде. Зато је неопходно извршити процену пропорционалности техничких и организационих мера које се могу имплементирати. Овај принцип има велику употребну вредност у области дигиталних друштвених мрежа. Како се наводи, „друштвене мреже би требало да подстичу уређивање профила на друштвеним мрежама на начин којим се штити приватност, на пример, да у старту ограниче могућност приступа профилу, тако да он није подразумевано (*by default*) доступан неодређеном броју лицу“. Принцип уграђене приватности значи да руковалац треба да примени адекватне мере искључиво над подацима о личности које су неопходне за остваривање сврхе обраде. Код овог принципа реч је о мерама које се „уграђују“ током процеса обраде, имајући на уму количину прикупљених података, обим њихове обраде, рок чувања и доступност другим лицима. Суштински најзначајнија последица овог принципа треба да буде сигурност од аутоматске доступности података о личности неодређеном броју лица. Посматрајући из друге перспективе, лице на које се подаци односе треба да одреди да ли ће своје податке поделити са већим одређеним или неодређеним кругом лица. Пример имплементације принципа уграђене приватности је употреба псеудонимизације (замене података о личности подложне идентификацији елементима који се не могу указати о ком лицу је реч) или енкрипције (кодирање порука електронске комуникације тако да само лице које је послало поруку и прималац могу јасно да је разумеју). Највише пажње поштовању ових принципа треба да посвете они који производе рачунарске системе и програме, будући да се у овим областима унапред могу поставити одређена подешавања којима се утиче на приватност грађана[48].

[48] С. Андоновић, Д. Прља, *op. cit.,* стр. 126-127.

IV МЕХАНИЗМИ ЗАШТИТЕ ОД ПОВРЕДЕ ПОДАТАКА О ЛИЧНОСТИ

У правном систему Републике Србије, али и у оквиру стандарда успостављених у Европској унији, механизми заштите од повреде података о личности обухватају низ мера које руковаоци и обрађивачи морају спровести у складу са законским обавезама. Ови механизми укључују законску одговорност руковаоца и обрађивача, спровођење процене утицаја на заштиту података, именовање службеника за заштиту података у одређеним случајевима, обавештавање надлежних органа, али и лица на које се подаци односе о повреди података, као и вођење евиденције радњи обраде. Поред тога, посебну улогу у обезбеђивању заштите података и превенције повреда има и Повереник за информације од јавног значаја и заштиту података о личности, чија надзорна и саветодавна функција представља један од кључних фактора у спречавању и контроли повреда података о личности.

1. Улога руковаоца и обрађивача

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[49]. Дакле, у одређеним ситуацијама, законодавац може директно да одреди која је сврха обраде података (нпр. заштита јавног здравља, вођење казнене евиденције), на који начин се подаци морају обрађивати (нпр. у ком систему, колико дуго, коме се смеју прослеђивати), као и ко ће бити руковалац (нпр. дом здравља, банка, АПР), односно који критеријуми морају бити испуњени да би неко имао ту улогу у обради података о личности. То значи да ће у великом броју ситуација руковаоци сами морати да процене да ли испуњавају законске критеријуме[50]. Ако два или више руковаоца заједнички одређују сврху и начин обраде, они се сматрају заједничким руковаоцима[51].

Одредити сврху обраде података о личности значи одредити разлог због кога се прикупљају или обрађују подаци грађана. Одредити начин обраде података о личности значи донети одлуку о томе како ће се користити прикупљени подаци[52].

[49] Чл. 4 став 1 тачка 8 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[50] С. Андоновић, Д. Прља, *op. cit.,* стр. 156.
[51] Чл. 43 став 1 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[52] С. Андоновић, Д. Прља, *op. cit*., стр. 156.

Обрађивач је физичко или правно лице, односно орган власти који обрађује податке о личности у име руковаоца[53]. Модерно доба са собом носи један тренд у коме су услуге обрађивача све траженије. Данас се услуге аутсорсују (енг. *outsourcing*) односно преносе комплетно обрађивачима, такође услуге клауда (енг. *cloud services*) и индустрија 4.0. су само од неких услуга које углавном обављају обрађивачи. Мора се нагласити да је обрађивач у ланцу одговорности заштите података само могућност и ствар избора руковалаца. Дакле обрађивач није нужни учесник у обради података о личности, пошто руковалац може део или читаву обраду података пренети обрађивачу (спољном или екстерном пружаоцу услуга). Притом је од суштинског значаја да обрађивач делује у име и искључиво по налогу руковаоца (чл. 29 ОУЗП). Уз то обрађивач не сме одлучивати о сврси и средствима обраде података[54].

Закон о заштити података о личности прописује бројне обавезе руковаоца, а које се, у зависности од тога да ли се односе на све или само на поједине руковаоце, могу поделити на опште и посебне обавезе. Опште обавезе се односе на све руковаоце и обухватају пре свега обавезу примене свих законом прописаних начела обраде података, као што су: начело законитости, поштења и транспарентности, начело ограничености сврхе обраде, начело сразмерности, односно минимизације обраде података, начело тачности података, начело ограниченог чувања података, начело безбедности података и начело одговорности. Поред тога, у опште обавезе се убрајају и обавеза руковаоца да поступа по захтевима лица на која се подаци односе[55], да даје обавештења о обради[56], као и да омогући остваривање права лица на која се подаци односе[57].

Поред општих обавеза, поједини руковаоци имају посебне обавезе које су последица било врсте руковаоца, било података који се обрађују или начина њихове обраде. Пре свега, када обраду врши обрађивач у име и по налогу руковаоца, руковалац је обавезан да закључи посебан уговор о обради у складу са чланом 45 став 3 Закона о заштити података о личности, а којим се дефинише предмет, трајање, природа и сврха обраде, врста података, као и обавезе о права руковаоца. Поред тога, руковалац је дужан да води евиденције радњи обраде, у складу са чланом 47 Закона о заштити података о личности,

[53] Чл. 4 став 1 тачка 9 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[54] А. Дилигенски, Д. Прља, Д. Церовић, *Право заштите података ГДПР*, Београд, 2018, стр. 71.
[55] Чл. 21 и 22 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[56] Чл. 23 и 24 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[57] Чл. 26-40 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

а уколико је реч о надлежним органима који обраду врше у посебне сврхе, чланом 48 предвиђено је и бележење сваке појединачне радње обраде приликом употребе система аутоматске обраде, што омогућава ревизију и контролу поступања. У случају повреде података о личности, члан 52 прописује обавезу руковаоца да без одлагања, а најкасније у року од 72 сата, обавести Повереника, као и лице на које се подаци односе у случају повреде високог ризика. Превентивни карактер има обавеза из чланова 54 и 55, а која се односи на спровођење процене утицаја на заштиту података у ситуацијама када одређени вид обраде, нарочито уз примену нових технологија, може проузроковати висок ризик по права и слободе појединаца. У складу са тим, у појединим случајевима неопходно је именовање лица за заштиту података у складу са члановима 56-58 Закона, чија улога је да обезбеди усаглашеност процеса обраде са законом и да делује као контакт тачка са надзорним органом. Даљи инструмент саморегулације представља доношење и придржавање кодекса поступања од стране удружења и других субјеката који представљају групе руковаоца или обрађивача, а у складу са чланом 59, а којим се у одређеним секторима унапређују стандарди усклађености. Коначно, посебне обавезе настају и у контексту међународног преноса података, при чему руковалац мора обезбедити да се такви преноси врше само у складу са Законом, односно уз примену одговарајућих заштитних мера и поштовање права лица на које се подаци односе.

На обрађиваче се такође односи обавеза поштовања основних начела обраде података о личности. То подразумева да би уопште дошло до ангажовања обрађивача и да би он могао да обавља активности обраде, неопходно је да постоји неки од законских основа обраде података[58].

У погледу избора обрађивача, руковалац је у обавези да изабере таквог обрађивача, који ће понудити довољне гаранције у виду одговарајућих техничких и организацијских мера пре свега у циљу заштите права појединаца (видети чл. 28 ст. 1 ОУЗП). Као критеријуми за процену подобних обрађивача могу се узети: стручно знање, поузданост, ресурси, спровођење техничких и организационих мера пре свега у погледу сигурности обраде података (у.т.р. 81 ОУЗП)[59].

[58] R. Bogendorfer, Datenschutz-Grundverordnung; in: Knyrim R., (ed.), *Datenschutzrecht*, Vienna, 2016, pp. 172-174.
[59] А. Дилигенски, Д. Прља, Д. Церовић, *op. cit*., стр. 74.

2. Процена утицаја на заштиту података о личности

Процена утицаја на заштиту података, као инструмент за процену ризика развијен у оквиру Опште уредбе о заштити података, служи за управљање ризицима повезаним са обрадом података о личности (у ширем смислу: заштитом приватности). У том контексту, процена утицаја на заштиту података подразумева идентификовање, вредновање и мерење релевантних фактора који се односе на управљање ризицима и процену њиховог интензитета[60]. Дакле, овај институт је први пут изричито уведен као законска обавеза у Општој уредби о заштити података, а касније је преузет у домаће законодавство кроз Закон о заштити података о личности. Његова суштина огледа се у томе да руковалац, пре започињања обраде која употребом нових технологија и узимајући у обзир природу, обим, околности и сврху, може проузроковати висок ризик за права и слободе физичких лица, мора извршити процену утицаја и потенцијалних последица које би таква обрада имала по лица чији се подаци обрађују, а све како би минимизовао могуће штетне ефекте. Оваква процена представља не само инструмент за постизање правне усклађености, већ и средство управљања ризиком и јачања транспарентности у обради података.

Обавезност процене утицаја јавља се у случају системске и свеобухватне процене стања и особина физичког лица код аутоматизоване обраде (што подразумева и профилисање) која резултира доношењем одлуке од значаја за правни положај појединца. Такође, процена утицаја на заштиту података о личности обавезна је код обраде посебних врста података о личности, као и података о личности у вези са кривичним пресудама и кажњивим делима, као и код системског надзора над јавно доступним површинама[61].

Поред ових, законом дефинисаних случајева, процена утицаја се, на основу Одлуке Повереника[62] обавезно врши и у следећим случајевима:

1) приликом обраде података о личности деце и малолетника у сврху профилисања, аутоматизованог одлучивања или за маркетиншке сврхе,

[60] F. Zarrabi, I. Wagner, E. Boiten, Changes in Conducting Data Protection Risk Assessment: Before and After GDPR implementation, *Proceedings on Privacy Enhancing Technologies*, No. 4, Vol. 2023, pp. 7.
[61] С. Андоновић, Д. Прља, *op. cit.,* стр. 160.
[62] Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника за информације од јавног значаја и заштиту података о личности, *Службени гласник РС*, бр. 45/2019.

2) код употребе нових технологија или технолошких решења за обраду података о личности или са могућношћу обраде података о личности који служе за анализу или предвиђање економске ситуације, здравља, склоности или интересовања, поузданости или понашања, локације или кретања физичких лица,
3) приликом обраде података о личности на начин који укључује праћење локације или понашања појединца у случају системске обраде података о комуникацији насталих употребом телефона, интернета или других средстава комуникације,
4) код обраде биометријских података у циљу јединствене идентификације запослених од стране послодавца и у другим случајевима обраде података о личности запослених од стране послодавца употребом апликација или система за праћење њиховог рада, кретања, комуникације и сл.,
5) при обради података о личности укрштањем, повезивањем или провером подударности из више извора,
6) у случајевима обраде посебних врста података о личности у сврху профилисања или аутоматизованог одлучивања.

Према Одлуци Повереника, руковалац је обавезан да изврши процену утицаја на заштиту података о личности и у другим случајевима 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.

Уколико процена утицаја на заштиту података о личности, која је спроведена у складу са чланом 54 Закона и Одлуком Повереника, покаже да намераване радње обраде могу довести до високог ризика по права и слободе појединаца уколико се не предузму мере за умањење таквог ризика, руководилац је у обавези да, пре отпочињања обраде, затражи од Повереника мишљење[63].

3. Именовање лица за заштиту података о личности

Институт лица за заштиту података о личности никада раније није постојао у српском законодавству. Он је у наш правни систем први пут уведен новим Законом о заштити података о личности из 2018. године, а по узору на европску праксу и регулативу.

[63] Чл. 55 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

Лице за заштиту података о личности је појединац који је у оквиру организације задужен за обезбеђивање усклађености са прописима о заштити података, едукацију и друге повезане задатке. Често представља општу контакт тачку унутар организације за питања у вези са обрадом података о личности[64]. Лице за заштиту података о личности може бити физичко лице које је стручно оспособљено за вршење ове изузетно специфичне функције, које поседује релевантно искуство, те поступа непристрасно, независно и без спољашњих утицаја у обављању послова који су законом прописани као дужности лица за заштиту података о личности. Уопште узев, лице за заштиту података о личности помаже у раду организације или лицу код кога је именовано, у вези са ефикасном и правилном применом општих правних норми које се односе на заштиту података о личности. Ово лице има превасходно консултативну, едукациону и усмеравајућу функцију, па његово именовање не ослобађа одговорности руковаоца за обраду података о личности[65].

Закон је именовање лица за заштиту података о личности у одређеним случајевима оставио као могућност руковаоца и обрађивача, али у одређеним случајевима је ово именовање прописано као њихова обавеза. Руковаоци и обрађивачи који немају обавезу именовања лица за заштиту података, али желе да подигну ниво усклађености са прописима и унапреде праксу заштите података у оквиру својих организација, добровољно именују лице за заштиту података као део шире стратегије управљања ризиком и јачања поверења лица чије податке обрађују. Оваква пракса се посебно препоручује у организацијама које обрађују мање количине података, али у контексту ”осетљивих” делатности (као што су образовање, ИТ услуге), као и у оним организацијама које стреме високим стандардима транспарентности и корпоративне одговорности. Са друге стране, руковалац и обрађивач дужни су да одреде лице за заштиту података о личности ако се:

1) обрада врши од стране органа власти, осим ако се ради о обради коју врши суд у сврху обављања његових судских овлашћења;

[64] P. Lambert, *op. cit*., pp. 4.
[65] С. Андоновић, Лице за заштиту података о личности у правном систему Србије, у: Андоновић С., Прља Д., Дилигенски А. (ур.), *Заштита података о личности у Србији*, Београд, 2020, стр. 118.

2) основне активности руковаоца или обрађивача састоје у радњама обраде које по својој природи, обиму, односно сврхама захтевају редован и систематски надзор великог броја лица на које се подаци односе;
3) основне активности руковаоца или обрађивача састоје у обради посебних врста података о личности (расно или етничко порекло, политичко мишљење, верско или филозофско уверење или чланство у синдикату, генетски подаци, биометријски подаци у циљу јединствене идентификације лица, подаци о здравственом стању или подаци о сексуалном животу или сексуалној оријентацији физичког лица) или података о личности у вези са кривичним пресудама и кажњивим делима, у великом обиму[66].

Прво, органи јавне власти имају обавезу именовања лица за заштиту података о личности. Под органима власти треба подразумевати све државне органе, органе територијалне аутономије и јединица локалне самоуправе, али и јавна предузећа, установе и друге јавне службе, затим организације и друга правна или физичка лица која врше јавна овлашћења. Дакле, под органима власти подразумевају се не само органи државне управе, већ и они органи који представљају део тзв. недржавне (јавне) управе, којима управни послови не представљају основну делатност, али те послове обављају на основу одговарајућих јавних овлашћења. Иако се могу одредити као органи власти, за судове не важи обавеза именовања лица за заштиту података о личности, али само у оним ситуацијама који се односе на обраду података у циљу обављања послова из судске надлежности. Логиком ствари, сматрамо да се обавеза именовања лица за заштиту података ипак односи на судове у погледу њихових административних послова и задатака, оних који се тичу рада судске управе, који нису у непосредној вези са судијском функцијом, већ су превасходно административног карактера.[67].

Друга два случаја у којима је прописана обавеза именовања лица за заштиту података о личности зависе од основних активности руковаоца и обрађивача. Уколико се основне активности руковаоца или обрађивача састоје од редовног и систематског надзора великог боја лица, они су дужни да именују лице за заштиту података о личности, у циљу превенције могућих повреда података и умањења потенцијалних ризика по права и слободе лица чији се подаци обрађују. Међутим, ни српски Закон о заштити података о

[66] Чл. 56 став 2 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[67] С. Андоновић, Лице за заштиту података о личности у правном систему Србије, *op. cit*., стр. 118-119.

личности, а ни европска Општа уредба о заштити података о личности, нису дали прецизно образложење шта се то подразумева под ”редовним и систематским надзором”. Детаљније образложење ових појмова проналазимо у Смерницама о лицима за заштиту података Радне групе 29, која појам ”редовно” тумачи тако да се активности надзора одвијају континуирано или у одређеним интервалима током одређеног временског периода, да се понављају у унапред одређеним временским терминима или да се одвијају стално или периодично. Радна група 29 појам ”систематски” тумачи тако да се надзор спроводи у складу са одређеним системом, да је унапред планиран, организован или методичан, да се спроводи као део општег плана прикупљања података, или да се извршава у оквиру одређене стратегије. Примери активности које могу представљати редован и систематски надзор субјеката података укључују: управљање телекомуникационом мрежом, пружање телекомуникационих услуга, ретаргетирање путем електронске поште, маркетиншке активности засноване на подацима, профилисање и оцењивање у сврху процене ризика (нпр. за кредитни рејтинг, одређивање осигуравајућих премија, спречавање превара, откривање прања новца), праћење локације, на пример, путем мобилних апликација, програми лојалности, оглашавање засновано на понашању корисника, надзор података о здрављу, кондицији и добробити путем уређаја који се носе на телу, надзор путем видео-надзорних система, повезани уређаји, као што су паметни бројила, паметна возила, системи за аутоматизацију дома и сл.[68].

Такође, уколико се основне активности руковаоца или обрађивача састоје у обради посебних врста података о личности, као и података о личности у вези са кривичним пресудама и кажњивим делима, у великом обиму, постоји обавеза именовања лица за заштиту података о личности. Како је законодавац и овде пропустио да дефинише шта се то подразумева под формулацијом ”велики обим” података, образложење смо принуђени потражити у смерницама Радне групе 29, а која препоручује да се следећи фактори узму у обзир када се процењује да ли се обрада врши у великом обиму:

1) број субјеката података на које се обрада односи – било као конкретан број или као пропорција у односу на релевантну популацију;
2) обим података и/или распон различитих врста података који се обрађују;

[68] Радна група члана 29. *Смернице о лицима за заштиту података, 16/EN, WP 243 rev. 01*, Брисел, 2016, стр. 8-9.

3) трајање или сталност активности обраде података;
4) географски обухват активности обраде.

На пример, обрада здравствених података хиљада пацијената у оквиру болничког система или системска обрада биометријских података запослених у великом привредном друштву, могла би се оправдано сматрати обрадом ”у великом обиму”. У пракси, процена великог обима мора се вршити контекстуално, у складу са природом активности и ризиком који обрада носи по права и слободе појединаца. У том смислу, именовање лица за заштиту података о личности представља не само законску обавезу, већ и превентивну меру управљања ризиком и јачања укупног система усклађености организације.

Лице за заштиту података о личности има најмање обавезу да:

1) информише и даје мишљење руковаоцу или обрађивачу, као и запосленима који врше радње обраде о њиховим законским обавезама у вези са заштитом података о личности;
2) прати примену одредби Закона о заштити података о личности, других закона и интерних прописа руковаоца или обрађивача који се односе на заштиту података о личности, укључујући и питања поделе одговорности, подизања свести и обуке запослених који учествују у радњама обраде, као и контроле;
3) даје мишљење, када се то затражи, о процени утицаја обраде на заштиту података о личности и прати поступање по тој процени, у складу са чланом 54 закона;
4) сарађује са Повереником, представља контакт тачку за сарадњу са Повереником и саветује се са њим у вези са питањима која се односе на обраду, укључујући и обавештавање и прибављање мишљења из члана 55 закона[69].

Руковалац или обрађивач дужан је да објави контакт податке лица за заштиту података о личности и достави их Поверенику. Повереник води евиденцију лица за заштиту података о личности. Евиденција садржи податке о руковаоцу, односно

[69] Члан 58 став 1 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

обрађивачу (име, презиме и адресу, односно назив и седиште) и податке о лицу за заштиту података о личности (име, презиме, адресу, имејл и број телефона)[70].

4. Обавештавање о повреди података о личности

Обавештавање Повереника о повреди података о личности, као и обавештавање лица на које се подаци односе о повреди података, представљају нове институте у домаћем праву. Ови институти имају за циљ брзо и ефикасно деловање у случају повреде података о личности[71].

Руковалац је дужан да без непотребног одлагања, а ако је то могуће, најкасније у року од 72 сата од тренутка сазнања за повреду података, обавести Повереника о повреди која је такве природе да може да проузрокује ризик по права и слободе физичких лица. Уколико руковалац није испоштовао овај рок, он мора Поверенику дати образложење разлога таквог закашњења. Такође, и обрађивач има обавезу да без одлагања обавести руковаоца чим сазна за повреду података о личности. Обавештење упућено Поверенику мора да садржи најмање следеће елементе:

1) опис природе повреде, укључујући врсту података, приближан број лица на која се подаци односе и број података који су обухваћени повредом;
2) име и контакт податке лица за заштиту података о личности, или алтернативне податке за контакт;
3) опис могућих последица повреде;
4) опис мера које је руковалац предузео или предложио ради ублажавања последица повреде.

Поред обавезе обавештавања Повереника, руковалац има обавезу и да документује сваку повреду, и то тако што ће укључити све чињенице о повреди и самом инциденту, његовим последицама и предузетим мерама, како би Повереник могао да процени његову усаглашеност са законским обавезама[72].

Када је у питању обавештавање самих лица чији су подаци повређени, руковалац је у обавези да, уколико повреда може да произведе висок ризик по права и слободе

[70] Члан 2 Правилника о обрасцу и начину вођења евиденције лица за заштиту података о личности, *Службени гласник РС*, бр. 40/2019.
[71] С. Андоновић, Д. Прља, *op. cit.,* стр. 159.
[72] Члан 52 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

физичких лица, без непотребног одлагања обавести та лица. Обавештење мора бити формулисано јасно и разумљиво и мора садржати најмање:

1) опис природе повреде података,
2) контакт податке лица за заштиту података,
3) опис могућих последица повреде,
4) опис мера које су предузете или предложене.

Закон предвиђа и одређене изузетке од обавезе директног обавештавања лица, као што су: ситуације када је обезбеђена примена ефикасних мера техничке и организационе заштите (нпр. енкрипција), када су накнадно предузете мере које елиминишу ризик, као и ситуације у којима би директно обавештавање било несразмерно сложено или скупо, у којима је дозвољено јавно или на други начин објавити обавештење[73].

Иако је законска регулатива јасно дефинисала обавезу обавештавања о повреди података о личности, у пракси се јављају бројни изазови приликом њеног извршења. Први изазов односи се на процену да ли повреда података заиста носи ”ризик” или ”висок ризик” по права и слободе појединаца, што је субјективна и често правно неодређена процена. У недостатку јасних методологија и смерница, постоји ризик или од непотребног обавештавања (претерана реакција), или од неблаговременог поступања (недовољна реакција). Други значајан изазов је организациона (не)спремност руковалаца. Многи руковаоци немају успостављене адекватне интерне процедуре, обучено особље или техничка средства за брзу идентификацију и процену повреде, као ни за прикупљање података неопходних за састављање обавештења. Такође, комуникација између обрађивача и руковалаца често није довољно ефикасна, што доводи до кашњења у пријављивању повреде.

5. Евиденција радњи обраде

Евиденција радњи обраде представља један од основних инструмената који обезбеђује руковаоцима и обрађивачима да поступају у складу са начелом законитости и транспарентности, као и начелом одговорности у обради података о личности. Сврха

[73] Члан 53 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

ове евиденције јесте да обезбеди преглед свих активности обраде података унутар једног система, као и да олакша контролу, како интерну тако и од стране надзорног органа, односно Повереника за информације од јавног значаја и заштиту података о личности.

Сваки руковалац и сваки обрађивач који запошљава више од 250 лица има обавезу да води евиденцију радњи обраде. Ова обавеза се примењује и на организације које, иако имају мање од 250 запослених, врше обраду која може проузроковати ризик по права и слободе појединаца, ако обрада није повремена, већ се врши континуирано и системски, ако врше обраду посебних врста података или података у вези са кривичним осудама, кажњивим делима и мерама безбедности.

Евиденција радњи обраде коју води руковалац мора да садржи најмање следеће информације:

1) име и контакт податке руковаоца, као и евентуалног заједничког руковаоца, представника руковаоца и лица за заштиту података;
2) сврха обраде;
3) опис категорија лица на које се подаци односе и категорија података о личности;
4) категорије прималаца којима су подаци откривени или ће бити откривени;
5) податке о преносу података у другу државу или међународну организацију;
6) рокове чувања података, када је рок одређен;
7) опис техничких и организационих мера заштите, уколико је то могуће.

Са друге стране, обрађивач је дужан да води евиденцију која садржи:

1) име и контакт податке обрађивача и сваког руковаоца у чије име поступа;
2) врсти обрада које обавља у име сваког руковаоца;
3) евентуалне преносе података у треће земље или међународне организације;
4) опис заштитних мера, ако је то могуће.

Ова евиденција може се водити у писаној или електронској форми, а мора бити доступна Поверенику на увид, на његов захтев[74].

[74] Члан 47 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

6. Улога Повереника за информације од јавног значаја и заштиту података о личности у превенцији повреда података

Повереник за информације од јавног значаја и заштиту података о личности представља независни државни орган, чија је основна улога заштита основних права и слобода физичких лица у вези са обрадом података о личности. Лице које је именовано на функцију Повереника дужно је да своје дужности обавља самостално и независно, и не сме примати нити тражити упутства од било ког субјекта. Исто тако, не сме обављати било коју другу јавну или политичку функцију, нити бити у радном односу на другом месту. Повереник се бира из реда лица која уживају углед стручњака специјализованог за заштиту људских права. Именује га Народна скупштина на период од седам година[75]. Повереник има широка овлашћења и надлежности, од саветодавних и едукативних до инспекцијских и корективних, с циљем превенције, контроле и санкционисања због извршених повреда података о личности.

У смислу превенције повреда података о личности, улога Повереника се реализује кроз више кључних функција. Он има обавезу да подиже свест јавности о ризицима, правилима, мерама заштите и правима у области обраде података, с посебним фокусом на заштиту података о малолетним лицима. У пракси се ово реализује кроз разне семинаре, јавне кампање и објављивање стручних водича и модела докумената. Повереник такође даје мишљења Народној скупштини, Влади и другим органима власти у погледу законских и подзаконских аката који утичу на заштиту података о личности, те на тај начин учествује у превентивној заштити. Лица на која се подаци односе могу се обратити Поверенику у случају сумње на повреду података. Повереник има дужност да поступа по таквим притужбама, утврди чињенично стање и обавести подносиоца о исходу. Када постоји ризик од незаконите обраде, Повереник може издати упозорење или мишљење у писаној форми, а у којем указује на могуће последице намераваних радњи. Оваква мера има изузетно превентивни карактер, јер омогућава рано отклањање неправилности.

Поред ових саветодавних и едукативних овлашћења усмерених на превенцију повреда, Повереник је овлашћен и да врши инспекцијски надзор над применом закона,

[75] D. V. Popović, The Pivotal Role of DPAs in Digital Privacy Protection: Assessment of the Serbian Protection Mechanism*;* in: G. Halmai, P. Bárd (ed.), *Liberty and Security in Europe – LIVe 4*, Budapest, 2022, pp. 139-140.

да проверава усаглашеност обраде са прописима, изриче мере и по потреби издаје прекршајне налоге. Још један важан аспект превенције јесте активна улога Повереника у праћењу савремених технологија и пословних пракси од значаја за обраду података, чиме се омогућава правовремена реакција на нове ризике. Такође, Повереник води и евиденцију о лицима за заштиту података, као и интерну евиденцију о повредама закона и мерама које су предузете, што представља значајан извор података за анализу трендова и усмеравање превентивне политике[76].

Узимајући у обзир све претходно наведено, улога Повереника у превенцији повреда података о личности има суштински значај и доприноси изградњи ефикасног и одрживог система. Као независни орган, Повереник делује на више нивоа, при чему његова интервенција има и реактивни и проактивни карактер. Због тога је Повереник кључна институционална карика која омогућава спровођење законских стандарда у пракси и доприноси стварању правне и организационе културе у којој се заштита података о личности посматра као кључни фактор у обезбеђењу поштовања људских права.

7. Техничке, организационе и кадровске мере заштите

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, руковалац и обрађивач спроводе одговарајуће техничке, организационе и кадровске мере како би достигли одговарајући ниво безбедности у односу на ризик[77]. Ове мере представљају кључни инструмент у спречавању, откривању и ублажавању последица неовлашћене обраде, губитка, измене или приступа подацима о личности.

Техничке мере укључују примену информационих и комуникационих технологија ради заштите података. Ни српски Закон о заштити података о личности, а ни савремени прописи широм света, не пружају прецизне дефиниције техничких мера нити јасна упутства о начину њихове имплементације, већ остављају та питања отвореним за тумачење. Разлог за технолошку неутралност лежи у жељи да се обезбеди

[76] Члан 78 став 1 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[77] Члан 50 став 1 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

флексибилност регулаторних оквира и да се омогући прилагођавање будућем технолошком развоју. Техничке мере заштите обухватају нарочито:

1) примену енкрипције ради заштите података у току преноса и чувања;
2) имплементацију система контроле приступа и аутентикације (нпр. двофакторска аутентикација);
3) инсталацију и редовно ажурирање антивирусних програма, система за контролу мрежног саобраћаја (енг. *firewall*), система за откривање и/или спречавање упада у информационе системе;
4) правовремено ажурирање софтвера;
5) одржавање резервних копија;
6) планови за опоравак у случају инцидента.

Организационе мере подразумевају усвајање интерних процедура, политика и примену механизама управљања подацима унутар самих организација које врше обраду података. Њихова сврха је да се омогући законита, транспарентна и контролисана обрада података. Основна мера је доношење интерног акта о заштити података о личности, којим треба да се уреде питања у вези са прикупљањем и обрадом података, безбедношћу података о личности, обавештавањем о начину остваривања права у вези са обрадом и заштитом података, приступом подацима о личности и одговорношћу за њихову незакониту обраду и употребу, као и вођењем евиденције активности обраде за сваку збирку података[78]. Поред ове мере, организационе мере заштите нарочито обухватају:

1) редовно процењивање ризика и ревизију безбедносних мера;
2) склапање уговора са обрађивачима којима се уређују обавезе у погледу заштите података;
3) дефинисање овлашћења и нивоа приступа подацима о личности за све актере у обради података.

Кадровске мере имају за циљ да обезбеде да особље које има приступ подацима буде адекватно обучено и одговорно у свом поступању. Овај вид мера нарочито обухвата:

[78] Đ. Krivokapić, D. Krivokapić, I. Todorović, S. Komazec, Mapping Personal Data Flow and Regulatory Compliance in Serbian Public Institutions *Management: Journal of Sustainable Business and Management Solutions in Emerging Economies*, no. 80, Vol. 21, pp. 6.

1) редовну едукацију запослених о обавезама у погледу заштите података;
2) обавезу поверљивости, дефинисану уговором или интерним актом;
3) именовање лица за заштиту података, уколико је то законом прописано као обавеза или је потребно с обзиром на природу обраде;
4) примену дисциплинских мера у случају кршења интерних политика у области заштите података.

Сви наведени типови мера морају бити адекватни у односу на ризик који свака конкретна обрада података са собом носи. Зато се препоручује коришћење модела процене ризика или процене утицаја на заштиту података, посебно у случајевима обраде која може изазвати висок ризик по права и слободе лица. Циљ је да се обезбеди ”уграђена и подразумевана заштита података” (енг. *privacy by design, privacy by default*), у складу са савременим прописима и технолошким стандардима.

V ПРАВНЕ ПОСЛЕДИЦЕ ПОВРЕДЕ ПОДАТАКА О ЛИЧНОСТИ

Свако физичко лице ужива право на заштиту података о личности. Ово право зајемчено је првенствено Уставом Републике Србије, а уставне одредбе су детаљније разрађене Законом о заштити података о личности. У случају да дође до незаконите обраде или другог облика повреде података о личности, правна одговорност се може испољити у више облика: грађанскоправна одговорност која се огледа у обавези накнаде материјалне и нематеријалне штете коју је лице претрпело због повреде података о личности, као и прекршајна и кривичноправна одговорност за теже и свесно учињене повреде података о личности.

1. Грађанскоправна одговорност

Грађанскоправна одговорност у случају повреде података о личности заснива се на општем начелу одговорности за штету. Лице које је претрпело материјалну или нематеријалну штету због повреде одредаба Закона о заштити података о личности Републике Србије, има право на новчану накнаду ове штете од руковаоца, односно

обрађивача који је штету проузроковао[79]. Руковалац одговара за штету коју је причинио својим незаконитим поступањем или пропуштањем да поступи у складу са законским обавезама, али исто тако он одговара и за поступке обрађивача кога је ангажовао, осим ако докаже да ни на који начин није одговоран за настанак такве штете. Са друге стране, обрађивач одговара само ако није поступао у складу са обавезама прописаним Законом о заштити података о личности, које се односе непосредно на њега или кад је поступао изван упутстава или супротно упутствима руковаоца[80].

Такође, Законом о облигационим односима прописано је да свако има право захтевати од суда или другог надлежног органа да нареди престанак радње којом се повређује интегритет људске личности, личног и породичног живота и других права његове личности. Закон даље прописује да суд, односно други надлежни орган, може наредити престанак радње под претњом плаћања извесне новчане своте, одређене укупно или по јединици времена, у корист повређеног[81].

Закон о облигационим односима предвиђа могућност накнаде штете у случају повреде права личности, али не помиње личне податке. Код повреде права личности по правилу ће бити реч о нематеријалној штети[82]. Нематеријална штета представља повреду личних добара неког лица, која се огледа у наношењу другоме физичког или психичког бола или страха[83]. Међутим, ту се отвара питање накнаде нематеријалне штете настале повредом личних података. Наиме, повреда (злоупотреба) одређених личних података не мора имати за последицу претрпљени физички или психички бол односно страх. У случају повреде личних података, ипак може настати одређена штетна последица, која не мора бити непосредно видљива. У недостатку судске праксе, можемо перципирати случај у коме су нарочито осетљиви подаци одређеног лица учињени јавним, што је већ само по себи негативна последица за лице о чијим подацима је реч. Етничко порекло, вероисповест и здравствено стање одређеног лица само су неки од личних података

[79] Члан 86 став 1 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[80] Члан 86 став 3 и 4 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[81] Члан 157 Закона о облигационим односима, *Службени лист СФРЈ*, бр. 29/78, 39/85, 45/89 - одлука УСЈ и 57/89, *Службени лист СРЈ*, бр. 31/93, *Службени лист СЦГ*, бр. 1/2003 - Уставна повеља и *Службени гласник РС*, бр. 18/2020.
[82] Д. Прља, С. Андоновић, Накнада штете код повреде личних података; у: Петровић З., Чоловић В. (ур.), *Одговорност за штету, накнада штете и осигурање*, Београд-Ваљево, 2018, стр. 232.
[83] Члан 155 Закона о облигационим односима, *Службени лист СФРЈ*, бр. 29/78, 39/85, 45/89 - одлука УСЈ и 57/89, *Службени лист СРЈ*, бр. 31/93, *Службени лист СЦГ*, бр. 1/2003 - Уставна повеља и *Службени гласник РС*, бр. 18/2020.

чијом злоупотребом (чињење тих података доступним јавности) може настати последица за одређено лице (избегавање контакта са тим лицем, вређање, одбијање на конкурсима због здравственог стања, али под другим изговорима и сл.). У тим случајевима, штетна последица је већ настала самим објављивањем личних података, иако изостаје последица у виду претрпљеног бола или страха. Уз то, за злоупотребу личних података, у многим случајевима, не може се сазнати одмах по учињеној повреди, већ тек касније током времена. Разлог томе лежи у развоју технологије и проблематици праћења обраде података на компјутерских технологијама и системима. Дакле, прихваћена концепција накнаде нематеријалне штете само у случају претрпљеног физичког или психичког бола и страха не може у потпуности одговорити на ризике које прете повредом личних података[84]. Из тог разлога, нематеријална штета треба да буде надокнађена и онда када изостаје последица у виду претрпљеног физичког или психичког бола или страха, јер већ само нарушавање права на заштиту података о личности представља повреду личности.

За разлику од Закона о облигационим односима, који не предвиђа изричиту заштиту у случају повреде права на заштиту података о личности, Закон о заштити података о личности изричито уводи могућност накнаде нематеријалне штете, без условљавања постојањем последица у виду претрпљеног физичког или психичког бола или страха, или другог конкретног облика патње. На тај начин, овај закон у значајној мери превазилази ограничења традиционалне грађанскоправне одговорности за нематеријалну штету и одговара потребама савременог дигиталног друштва у коме је повреда података о личности често невидљива, са одложеним последицама и тешко доказива, али итекако реална.

2. Прекршајна одговорност

Ова врста одговорности има репресивни и превентивни карактер, с обзиром на то да се новчане казне примењују ради спречавања будућих неправилности у поступању са подацима о личности. Законом о заштити података о личности прописан је широк спектар прекршаја за које могу одговарати руковаоци и обрађивачи података, укључујући и одговорна физичка лица у правном лицу и предузетнике. Као прекршаји се квалификују, између осталог, обрада података супротно основним начелима обраде,

[84] Д. Прља, С. Андоновић, *op. cit*., стр. 233-234.

обрада без правног основа, незаконита обрада посебних категорија података о личности, повреда обавезе информисања лица на које се подаци односе, ускраћивање приступа подацима, пропуштање предузимања техничких и организационих мера заштите, као и незаконит пренос података у иностранство. Закон обухвата и прекршаје у вези са аутоматизованим одлучивањем, непоступањем по налозима Повереника, неименовањем лица за заштиту података, као и пропусте у вођењу евиденција радњи обраде и у поступцима процене утицаја. Поред тога, законом су санкционисани и мање тешки прекршаји, ко што су непружање тражених информација у предвиђеном року или непоштовање обавезе чувања професионалне тајне[85].

Одговорност могу сносити правна лица, одговорна лица у правном лицу, предузетници, као и физичка лица уколико је закон предвидео њихову прекршајну одговорност (нпр. лице за заштиту података о личности[86], Повереник, заменик Повереника и запослени у служби Повереника[87]).

Прописане новчане казне за правна лица су од 50.000 динара до 2.000.000 динара, а за одговорна физичка лица од 5.000 до 150.000 динара, у зависности од врсте и тежине прекршаја.

У пракси, Повереник подноси захтев за покретање прекршајног поступка када у поступку надзора утврди да је дошло до повреде закона. Иако је његова надлежност превасходно управна и корективна, прекршајне санкције служе као важан инструмент притиска, посебно у случајевима поновљених или тешких повреда података о личности.

3. Кривичноправна одговорност

Кривичноправна одговорност представља најстрожи облик правне последице повреде података о личности и примењује се када радње обраде добију карактер друштвено опасног понашања. У правном систему Републике Србије, основ за кривичноправну заштиту података о личности лежи у члану 146 Кривичног законика, који инкриминише неовлашћено прикупљање личних података. Према овом члану, ко податке о личности

[85] Члан 95 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[86] Члан 57 став 7 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[87] Члан 76 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

који се прикупљају, обрађују и користе на основу закона неовлашћено прибави, саопшти другом или употреби у сврху за коју нису намењени, казниће се новчаном казном или затвором до једне године. Истом казном казниће се и ко противно закону прикупља податке о личности грађана или тако прикупљене податке користи. Уколико ово дело учини службено лице у вршењу службе, запрећена је казна затвора до три године[88].

Поред кривичноправне одговорности физичких лица, у контексту повреде података о личности је значајно истаћи и то да се у српском правном поретку признаје и одговорност правних лица за кривична дела, у складу са Законом о одговорности правних лица за кривична дела. Одредба члана 2 ЗОПЛКД одређује круг кривичних дела за које правно лице може одговарати. Његова формулација показује како се српски законодавац определио за систем опште одговорности правног лица. Правно лице одговара за сва кривична дела из посебног дела Кривичног законика и споредног кривичног законодавства, ако су испуњени предвиђени услови за његову одговорност. Чини се да је интенција српског законодавца била да избегне „замку“ коју носи систем енумерације кривичних дела[89]. Дакле, правно лице одговара и за кривично дело неовлашћеног прикупљања личних података. Правно лице одговара за кривично дело које у оквиру својих послова, односно овлашћења учини одговорно лице у намери да за правно лице оствари корист. Одговорност правног лица постоји и ако је због непостојања надзора или контроле од стране одговорног лица омогућено извршење кривичног дела у корист правног лица од стране физичког лица које делује под надзором и контролом одговорног лица[90]. Такав приступ омогућава санкционисање системских пропуста унутар организација, као што су занемаривање процедура безбедности, недостатак надзора над обрадом података о личности или успостављање пословне праксе која толерише или охрабрује незакониту обраду података о личности, било кроз експлицитне инструкције или пропусте у организационој контроли.

Правном лицу се могу изрећи различите мере, као што су новчана казна, забрана обављања делатности, одузимање имовинске користи, јавна објава пресуде, па чак и укидање правног лица у најтежим случајевима. Ове мере имају и превентивну и

[88] Члан 146 Кривичног законика, *Службени гласник РС*, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 и 94/2024.
[89] М. Милошевић, *Одговорност правних лица за кривична дела*, (2012), стр. 143-144; преузето 25.6.2025. https://nardus.mpn.gov.rs/bitstream/handle/123456789/2601/Disertacija.pdf?sequence=4&isAllowed=y
[90] Члан 6 Закона о одговорности правних лица за кривична дела, *Службени гласник РС*, бр. 97/2008.

репресивну функцију, посебно у контексту све чешћих злоупотреба података о личности у дигиталном окружењу.

Иако се кривичноправна одговорност за повреду података о личности у пракси ретко реализује, њено постојање има значајну превентивну улогу јер указује на озбиљност повреде података о личности и ствара основ за реакцију у случајевима системских и тешких повреда.

VI УТИЦАЈ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ НА ПОВРЕДЕ ПОДАТАКА О ЛИЧНОСТИ: РИЗИЦИ И ИЗАЗОВИ КОЈИ ПРАТЕ ЊЕНУ ПРИМЕНУ

Савремене дефиниције углавном представљају вештачку интелигенцију као симулацију процеса људске интелигенције одговарајућим алгоритмом, кодом или техником уз помоћ машина или рачунарских система. Предмет проучавања вештачке интелигенције су заправо правила управљања тзв. интелигентним људским понашањима и стварање формалних модела ових понашања, уз помоћ рачунарских програма који ће симулирати ово понашање[91]. Идеја вештачке интелигенције јесте креирање машина које имају читав низ могућности за интелигентне акције које поседују људи, односно да се произведу машине које су свесне себе и аутономне на исти начин као људска бића (свети грал вештачке интелигенције). Алгоритам управља аутомобилом, анализира снимке камера са улица и препознаје лица, одлучује о додели социјалне помоћи, одлучује о додели кредита, доноси медицинску дијагнозу, управља снабдевањем струјом, водом, гасом, управља роботима, управља смртоносним снајпером или дроном и то све у готово потпуном правном вакуму. Право још увек није одговорило на адекватан начин на изазове које доносе нове технологије, а посебно изазове које доноси употреба вештачке интелигенције[92].

Развој и примена система заснованих на вештачкој интелигенцији такође убрзано мењају начин прикупљања, обраде и коришћења података о личности. Масовност обраде података, тешкоће у утврђивању правног основа, недостаци транспарентности алгоритама и немогућност потпуног остваривања контроле над подацима чине вештачку

[91] Д. Прља, Г. Гасми, В. Корач, *Вештачка интелигенција у правном систему ЕУ*, Београд, 2021, стр. 65.
[92] *ibid*., стр. 127.

интелигенцију изворoм специфичних изазова са становишта права на заштиту података о личности.

1. Аутоматизована обрада података и профилисање

Аутоматизована обрада података подразумева доношење одлука на основу алгоритама који обрађују податке о личности без директне људске интервенције и контроле. Посебан облик аутоматизоване обраде јесте профилисање, односно аутоматизована анализа личних карактеристика појединца, као што су склоности, понашање, интересовања, навике, економски статус или здравствено стање, ради предвиђања или категоризације. Оваква обрада носи значајне ризике по појединце, јер може довести до неправедног третмана, дискриминације или нетранспарентних одлука које могу имати озбиљне последице.

Лице на које се подаци односе има право да се на њега не примењује одлука донета искључиво на основу аутоматизоване обраде, укључујући и профилисање, ако се том одлуком производе правне последице по то лице или та одлука значајно утиче на његов положај. Ово правило има три изузетка, те је овај вид обраде дозвољен: када је аутоматизована обрада неопходна за закључење или извршење уговора, када је аутоматизована обрада заснована на закону, уз примену прописаних мера заштите, те када се врши на основу изричите сагласности лица на које се подаци односе[93].

Питање аутоматизоване обраде и профилисања је централно и у Акту о вештачкој интелигенцији Европске уније, који предвиђа експлицитну забрану такозваног ”социјалног бодовања”. Забрањено је стављање у употребу било ког система вештачке интелигенције чија је сврха евалуација или класификација појединца на основу његовог друштвеног понашања или личних особина, када таква класификација доводи до неповољног поступања према појединцу у друштвеним контекстима који нису повезани с контекстима у којима су подаци изворно генерисани или прикупљени, или поступања које је несразмерно или неоправдано у односу на понашање појединца[94]. Овом нормом се спречавају праксе где би системи вештачке интелигенције, на основу података из, на

[93] Члан 38 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[94] Члан 5 став 1 тачка ц Акта о вештачкој интелигенцији Европске уније, *Службени лист Европске уније,* бр. L 1689 од 12.7.2024. године.

пример, претраживања интернета или са друштвених мрежа, одређивали кредитну способност, погодност за запошљавање или за социјалне услуге. Такви механизми, чак и када не крше формалне одредбе о усклађености, подривају основне принципе фер и транспарентне обраде, као и људско достојанство. У том смислу, и национални и европски правни оквири указују да се аутоматизовано доношење одлука не сме посматрати као техничка појава, већ као правно релевантна активност која захтева прецизно нормативно регулисање и етичко усклађивање.

2. Биометријска обрада и надзор

Савремени системи вештачке интелигенције све више користе биометријске податке, као што су фацијална структура, отисци прстију, глас или геометрија шаке, ради идентификације и аутентикације, али неретко и ради надзора појединаца. Иако ова технологија често нуди многе предности у сфери безбедности, она у исто време подразумева и обраду најосетљивијих категорија података, односно оних података чија обрада подразумева високе ризике по права и слободе грађана. Посебно је проблематична масовна примена биометријског видео надзора у јавним просторима, што отвара питања легитимности, пропорционалности и транспарентности обраде.

У правном систему Републике Србије, биометријски подаци спадају у посебне врсте података о личности. Њихова обрада је дозвољена само изузетно, у следећим случајевима:

1) уколико је лице на које се подаци односе дало изричит пристанак за обраду за једну или више сврха обраде, осим ако је законом прописано да се обрада не врши на основу пристанка;
2) ако је обрада неопходна у циљу извршења обавеза или примене законом прописаних овлашћења руковаоца или лица на које се подаци односе у области рада, социјалног осигурања и социјалне заштите, ако је таква обрада прописана законом или колективним уговором који прописује примену одговарајућих мера заштите основних права, слобода и интереса лица на које се подаци односе;
3) када је обрада неопходна у циљу заштите животно важних интереса лица на које се подаци односе или другог физичког лица, ако лице на које се подаци односе физички или правно није у могућности да даје пристанак;

4) уколико се обрада врши у оквиру регистроване делатности и уз примену одговарајућих мера заштите од стране задужбине, фондације, удружења или друге недобитне организације са политичким, филозофским, верским или синдикалним циљем, под условом да се обрада односи искључиво на чланове, односно бивше чланове те организације или лица која имају редовне контакте са њом у вези са циљем организације, као и да се подаци о личности не откривају изван те организације без пристанка лица на које се односе;
5) ако се обрађују подаци о личности које је лице на које се они односе очигледно учинило јавно доступним;
6) када је обрада неопходна у циљу подношења, остваривања или одбране правног захтева или у случају кад суд поступа у оквиру своје надлежности;
7) уколико је обрада неопходна у циљу остваривања значајног јавног интереса одређеног законом, ако је таква обрада сразмерна остваривању циља, уз поштовање суштине права на заштиту података о личности и ако је обезбеђена примена одговарајућих и посебних мера заштите основних права и интереса лица на које се ови подаци односе;
8) ако је обрада неопходна у сврху превентивне медицине или медицине рада, ради процене радне способности запослених, медицинске дијагностике, пружања услуга здравствене или социјалне заштите, односно управљања здравственим или социјалним системима, на основу закона или на основу уговора са здравственим радником, ако се обрада врши од стране или под надзором здравственог радника или другог лица које има обавезу чувања професионалне тајне прописане законом или професионалним правилима;
9) када је обрада неопходна у циљу остваривања јавног интереса у области јавног здравља, као што је заштита од озбиљних прекограничних претњи здрављу становништва или обезбеђивање високих стандарда квалитета и сигурности здравствене заштите и лекова или медицинских средстава, на основу закона који обезбеђује одговарајуће и посебне мере заштите права и слобода лица на које се подаци односе, посебно у погледу чувања професионалне тајне;
10) као и онда када је обрада неопходна у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања и у статистичке сврхе, ако је таква обрада сразмерна остваривању циљева који се намеравају постићи, уз поштовање суштине права на заштиту података о личности и ако је обезбеђена примена

одговарајућих и посебних мера заштите основних права и интереса лица на које се ови подаци односе[95].

Поред наведених ограничења у погледу правног основа и сврхе обраде, као што је раније и наведено у овом раду, руковалац има обавезу да, пре започињања било какве обраде биометријских података која може да произведе висок ризик по права и слободе лица, изради процену утицаја на заштиту података о личности. Ова обавеза руковаоца има превентивну функцију и представља инструмент за идентификовање потенцијалних ризика, као и за дефинисање техничких и организационих мера које ће обезбедити законитост, транспарентност и безбедност обраде.

Када је реч о европском нормативном оквиру, Акт о вештачкој интелигенцији посебно препознаје биометријску обраду као високоризичну, те уводи потпуну забрану коришћења система који врше биометријску категоризацију појединаца у циљу извођења закључака о њиховој раси, политичким ставовима, верским уверењима, сексуалној орјентацији или чланству у синдикату. Оваква класификација се сматра проблематичном јер омогућава дискриминацију на основу осетљивих личних карактеристика појединаца. Једини изузетак од ове забране чини означавање или филтрирање законито прибављених биометријских скупова података, као што су слике, и то искључиво у контексту кривичног гоњења[96]. Даље, Акт о вештачкој интелигенцији строго забрањује употребу система за биометријску идентификацију у реалном времену у јавним просторима, у сврху кривичном гоњења, осим у експлицитно наведеним случајевима:

1) када се траже жртве отмице, трговине људима или сексуалног искоришћавања људи, као и код потраге за несталим лицима;
2) у циљу спречавања непосредне и конкретне опасности по живот или безбедност или код стварне претње од терористичког напада;
3) ради лоцирања осумњичених за тешка кривична дела за запрећеном казном од најмање 4 године затвора[97].

Упоређујући европски и српски правни оквир, јасно је да су оба правна система свесна потенцијалних ризика и штетности биометријске обраде података о личности, али се Акт

[95] Члан 17 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.
[96] Члан 5 став 1 тачка г Акта о вештачкој интелигенцији Европске уније, *Службени лист Европске уније,* бр. L 1689 од 12.7.2024. године.
[97] Члан 5 став 1 тачка х Акта о вештачкој интелигенцији Европске уније, *Службени лист Европске уније,* бр. L 1689 од 12.7.2024. године.

о вештачкој интелигенцији Европске уније одликује прецизнијим мерама превенције и забранама, док се српски пропис више ослања на општа начела и процену ризика. Из тог разлога, потреба за прецизирањем и нормативним унапређењем у домаћем праву постаје све актуелнија.

3. Проблем транспарентности и објашњивости алгоритама

Један од најзначајнијих изазова у примени система вештачке интелигенције приликом обраде података о личности јесте проблем недовољне транспарентности и ограничене објашњивости алгоритамских одлука. У ситуацијама у којима се аутоматизованим путем доносе одлуке које могу имати правне или фактичке последице по појединца (било да је реч о кредитној способности, приступу социјалним услугама, и слично) недостатак могућности јасног увида у логику одлучивања представља озбиљан ризик за остваривање основних права појединаца. Алгоритми, посебно они који користе дубоко машинско учење, често функционишу као ”црне кутије”, те је њихов начин рада тешко разумљив, чак и стручњацима који се баве развојем система вештачке интелигенције.

Управо због ових недостатака, Акт о вештачкој интелигенцији прописује да системи вештачке интелигенције високог ризика морају бити дизајнирани и примењени тако да обезбеде адекватан ниво објашњивости. Циљ није само техничка транспарентност, већ и обезбеђивање правне и функционалне разумљивости у погледу тога како систем доноси одлуке и какве последице из њих произлазе. Поред тога, прописана је обавеза достављања детаљног приручника за употребу, у коме се морају навести подаци о карактеристикама, ограничењима, тачности и безбедносним параметрима система, укључујући и информације о томе на основу којих улазних података је систем трениран, како се генеришу излазни подаци, и у којој мери их је могуће објаснити крајњем кориснику[98].

И у оквиру српског Закона о заштити података о личности, имплицитно се захтева транспарентност у случајевима аутоматизованог одлучивања, кроз обавезу да се лицу омогући да оспори одлуку, изнесе свој став и захтева људску интервенцију[99]. Ипак, у

[98] Члан 13 Акта о вештачкој интелигенцији Европске уније, *Службени лист Европске уније,* бр. L 1689 од 12.7.2024. године.
[99] Члан 38 став 3 Закона о заштити података о личности, *Службени гласник РС*, бр. 87/2018.

одсуству посебног акта који би обавезивао на техничку објашњивост алгоритма, овај стандард остаје више декларативан него извршив у пракси.

Због свега наведеног, транспарентност и објашњивост система вештачке интелигенције представљају не само технички, већ пре свега правни и етички изазов, који је од суштинског значаја за поверење јавности, заштиту приватности и одговорну употребу вештачке интелигенције.

VII СТУДИЈЕ СЛУЧАЈА

1. Повреда података у јавном сектору: пример МУП-а Републике Србије и биометријског надзора

У првој половини 2019. године, Министарство унутрашњих послова Републике Србије планирало је постављање великог броја паметних камера у Србији, а првенствено у Београду, опремљених технологијом за препознавање лица, у оквиру пројекта ”Safe City” реализованог уз подршку кинеске компаније ”Huawei”[100]. SHARE фондација и друге организације цивилног друштва су оштро критиковале ову меру, указујући да је планирана без јасног законског основа, јавне расправе и формално спроведене процене утицаја на заштиту података. Критика се посебно односила на недостатак процене утицаја на заштиту података о личности, која је према Закону о заштити података о личности обавезна у случајевима високоризичне обраде података попут масовне обраде биометријских података надзором у јавном простору.

У фебруару 2022. године, након притужби грађана услед најава употребе технологија за препознавање лица током протеста из новембра и децембра 2021. године, Повереник за информације од јавног значаја и заштиту података о личности је спровео инспекцијски надзор у МУП-у. Проверена је документација, техничке могућности уређаја ”HUAWEI EP 821” и начин употребе технологије. У налазу је утврђено да није активирана функција препознавања лица, те да уређаји, како је наведено, нису пласирани са биометријским софтвером[101]. Овај поступак је, међутим, само привремено одложио јавну дебату и није

[100] Support4Partnership, *The fight in Serbia over Chinese-style surveillance (Part One)*, (2022); преузето 1.7.2025. https://support4partnership.org/en/news/the-fight-in-serbia-over-chinese-style-surveillance-part-one

[101] Повереник за информације од јавног значаја и заштиту података о личности, *Повереник спровео поступак надзора у МУП, поводом сумњи на употребу технологије за препознавање лица (Facial*

решио тему нормативног и процесног усклађивања, а пре свега проблем недостатка процене утицаја на заштиту података о личности, као и недостатак законског оквира.

Овај случај илуструје неколико суштинских проблема:

1) нормативни вакуум у подзаконским актима МУП-а, који омогућавају потенцијалну злоупотребу технологије;
2) пропусти у практичној примени закона, због недостатка процене утицаја и јавне расправе; и
3) институционални отпор промени, иако је Повереник инсистирао на стриктном испуњењу законских и процедуралних предуслова.

Закључно, ова студија случаја указује да иако надзорна тела имају капацитете да реагују, ефикасна примена закона зависи како од јасно дефинисаних правних стандарда, тако и од политичке и институционалне воље да се они доследно спроводе.

2. Повреда података у приватном сектору: пример Ерсте банке и прикупљања здравствених података путем анкете о вакцинацији

У периоду пандемије вируса COVID-19, бројне организације су покушале да прилагоде своје интерне здравствене и безбедносне политике прикупљањем података о вакцинацији запослених. Међутим, један значајан случај у приватном сектору у Србији показао је како и у добрим намерама може доћи до повреде права на заштиту података о личности. Ради се о поступању Ерсте банке а.д. Нови Сад, која је током 2021. године спроводила анкету међу својим запосленима о статусу вакцинације против вируса COVID-19. Анкета је садржала питања о томе да ли је запослени вакцинисан (и у којој мери), да ли је прележао вирус, те какве су његове намере и ставови у вези са вакцинацијом. Иако је прикупљање статистичких података ради планирања здравствених мера можда било оправдано у ширем друштвеном контексту, Повереник је утврдио да су тим поводом прикупљани и лични подаци као што су име и презиме запослених, чиме је дошло до могућности повезивања запослених са њиховим одговорима, и то без јасног правног основа.

Recognition Technology), (2022); преузето 1.7.2025. https://www.poverenik.rs/sr-yu/saopstenja/3730-повереник-спровео-поступак-надзора-у-муп,-поводом-сумњи-на-употребу-технологије-за-препознавање-лица-facial-recognition-technology.html

Повереник је оценио да је обрада ових података представљала повреду више одредаба Закона о заштити података о личности, и то:

1) члана 12 став 1 Закона, јер није постојао законит основ обраде;
2) члана 17 став 1 Закона, будући да су се обрађивали подаци о здравственом стању без примене неке од изузетно прописаних законских основа;
3) као и члана 5 став 1 тачка 3 Закона, јер је обрада прекршила начело минимизације података, с обзиром на то да се жењена сврха могла постићи без идентификационих података запослених.

Иако је банка тврдила да је податке користила искључиво у сврху статистичке анализе ради утврђивања даљих превентивних мера, и да се подаци нису задржавали у облику који омогућава идентификацију запослених након попуњавања анкете, Повереник је закључио да је сама чињеница идентификације и прикупљања података у том облику представљала повреду закона. Као последица, Ерсте банци је изречена опомена, с обзиром на то да су подаци били обрисани након анализе, да није формирана трајна база података, као и да је извршена процена утицаја на заштиту података пре обраде, што је сведочило о намери руковаоца да поступа одговорно, упркос погрешној процени правног основа[102].

Овај случај јасно указује на то да ни епидемиолошка ситуација, ни интереси јавног здравља, не могу апсолутно оправдати обраду података без правног основа. Посебно је значајно што је обрада обухватала посебне врсте података, за које закон прописује рестриктиван режим. Студија такође отвара питања односа између права на приватност запослених и права послодавца да заштити здравље колектива, што је све актуелнија тема у европском праву у постпандемијском периоду.

3. Европски случај повреде података: Schrems II пресуда и последице за међународни пренос података

Један од најутицајнијих случајева у области заштите података о личности у Европској унији јесте пресуда Суда правде Европске уније у предмету Schrems II, донета 16. јула

[102] Повереник за информације од јавног значаја и заштиту података о личности. *Извештај о раду Повереника за информације од јавног значаја и заштиту података о личности за 2021. годину*, Београд, 2022, стр. 53-54.

2020. године[103]. Ова одлука поништила је ”Privacy Shield”, механизам који је омогућавао легитиман пренос података из Европске уније у САД, и тиме суштински изменила оквир за међународни пренос података.

Предметни спор је покренуо аустријски активиста Максимилиан Шремс, који је довео у питање правну сигурност трансфера података од стране Фејсбука (компаније Мета) у САД. Он је указао на то да закони САД-а, а нарочито у области обавештајног надзора (нпр. FISA - Foreign Intelligence Surveillance Act), не обезбеђују ниво заштите података еквивалентан оном који је прописан у праву Европске уније, посебно у смислу правних лекова и заштите основних права.

И заиста, пресудом Суда правде Европске уније у предмету Schrems II, суд је утврдио да механизам ”Privacy Shield” не пружа довољне гаранције у погледу правне заштите и да државни надзор у САД није пропорционалан, чиме се крше чланови 7, 8 и 47 Повеље о основним правима ЕУ. Стандардне уговорне клаузуле су остале на снази, али само под условом да пружају ефективан ниво заштите у пракси. То значи да руковаоци подацима морају вршити процену ризика у сваком конкретном случају и примењивати додатне мере (техничке, организационе и кадровске), ако је то неопходно. Надзорна тела држава чланица ЕУ имају овлашћење и обавезу да суспендују или забране трансфер података када се утврди да се адекватна заштита не може обезбедити.

Schrems II представља прекретницу у правној политици ЕУ у области међународног преноса података. Одлука је довела до правне несигурности за велики број компанија, нарочито у дигиталном сектору, јер више нису могле аутоматски заснивати своје трансфере на дотадашњим механизмима. Ово је иницирало развој нових стандардних клаузула од стране Европске комисије 2021. године, као и усвајање Data Privacy Framework-a (DPF)[104] у јулу 2023. године, који представља нови покушај стварања услова за безбедан пренос података између ЕУ и САД.

[103] Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, para. 201.
[104] Извршна одлука Комисије (ЕУ) 2023/1795 од 10. јула 2023. године, у складу са Уредбом (ЕУ) 2016/679 Европског парламента и Савета, о адекватном нивоу заштите личних података у оквиру ЕУ–САД оквира за приватност података (EU–U.S. Data Privacy Framework), саопштено под бројем документа C(2023) 4745, *Службени лист ЕУ*, L 191 од 14.7.2023, стр. 1–62.

4. Употреба вештачке интелигенције и повреда права на заштиту података о личности: пример Clearview AI

Америчка компанија Clearview AI развила је систем за препознавање лица који масовно прикупља биометријске податке без пристанка лица на која се подаци односе, користећи их за идентификацију лица, чак и на територији ЕУ. Систем се заснива на аутоматизованом прикупљању фотографија користећи технику познату као "web scraping", при чему се са различитих интернет платформи и друштвених мрежа преузимају јавно доступне фотографије, које се затим користе за формирање обимне базе података намењене алгоритамској, односно аутоматизованој, обради лица.

Надзорна тела за заштиту података о личности у више држава чланица Европске уније утврдила су да активности компаније Clearview AI представљају озбиљно кршење основних начела Опште уредбе о заштити података (ГДПР), укључујући недостатак правног основа за обраду, поступање супротно начелу транспарентности и повреду права на приступ подацима, као и незакониту обраду биометријских података. Француска надзорна агенција (Commission nationale de l'informatique et des libertés) издала је у новембру 2021. године формално наређење којим се компанији Clearview AI налаже обустава даље обраде и брисање података грађана Француске, утврдивши повреду више одредаба ГДПР-а, укључујући чланове 6, 12, 15 и 17. Услед одбијања сарадње, у априлу 2023. године компанији Clearview AI је изречена казна у износу од 5,2 милиона евра[105]. Сличан закључак изнео је и италијански орган за заштиту података (Garante), који је у марту 2022. године компанији Clearview AI изрекао новчану казну од 20 милиона евра, забранио даљу обраду података о личности на територији Италије и наложио брисање свих незаконито прикупљених информација, укључујући и биометријске податке[106].

Примери из праксе који се односе на поступање компаније Clearview AI представљају илустрован показатељ примене основних начела заштите података у оквиру правног поретка ЕУ. Утврђено је да је обрада фотографија лица без претходно прибављеног пристанка у супротности са чланом 6 Опште уредбе о заштити података, којим се прописује нужност постојања законитог правног основа за вршење било које радње

[105] European Data Protection Board, *The French SA fines Clearview AI EUR 20 million*, (2022); преузето 4.7.2025. https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en
[106] European Data Protection Board, *Facial recognition: Italian SA fines Clearview AI EUR 20 million,* (2022); преузето 4.7.2025. https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

обраде података о личности. Поред тога, аутоматизована обрада биометријских података без испуњења услова прописаних чланом 9 Опште уредбе, сматра се незаконитом, с обзиром на то да се ради о посебно осетљивој категорији података чија је заштита подигнута на виши ниво. Истовремено, у овим случајевима идентификовано је и кршење низа права лица на које се подаци односе, као што су право на приступ подацима, право на брисање, као и право на транспарентност обраде, у складу са одредбама чланова 12-17 Опште уредбе. Мере које су предузеле националне надзорне институције, укључујући изрицање новчаних казни, забрану даљег деловања и налоге за брисање података, потврђују способност и спремност регулаторних тела у оквиру ЕУ да ефикасно реагују на ризике које представљају системи вештачке интелигенције.

Случај Clearview AI представља репрезентативан пример потенцијалних повреда права на приватност у доба интензивног развоја и примене алгоритамских система. Иако је реч о компанији која формално делује ван територијалног домета Опште уредбе, њене активност имају директне правне последице унутар ЕУ, што илуструје екстериторијалну примену ГДПР-а. У контексту Републике Србије, која настоји да своје прописе усклади са европским стандардима, наведени случај може послужити као релевантан модел превентивног поступања и заштите грађана од неправилне обраде података од стране субјеката из приватног сектора, користећи модерне технологије и системе вештачке интелигенције.

VIII ЗАКЉУЧНА РАЗМАТРАЊА

Право на заштиту података о личности представља једно од кључних људских права у дигиталном добу, а његова ефикасна заштита све више добија на значају у контексту брзе технолошке трансформације и развијања нових метода обраде података. Анализом важећег правног оквира у Републици Србији, као и компарацијом са европским стандардима, нарочито са Општом уредбом о заштити података, утврђено је да постоје нормативне основе за адекватну заштиту, али да њихова примена у пракси постаје недоследна и изазовна у условима брзо променљивог окружења.

У овом раду је обрађен сложен феномен повреде података о личности, чији су узроци вишеструки, од техничких пропуста и људских грешака, до недовољне правне и

институционалне припремљености система. Уочено је да механизми превенције, као што су процена утицаја на заштиту података о личности, именовање лица за заштиту података о личности и вођење евиденција радњи обраде, имају кључну улогу у спречавању инцидената, али се и даље недоследно примењују. У том контексту, улога Повереника показала се као централна за функционисање система заштите, како у саветодавном, тако и у инспекцијском и корективном смислу.

Истовремено, све већи ризици од злоупотребе података у условима примене система заснованих на вештачкој интелигенцији додатно усложњавају ову правну област. Аутоматизовано одлучивање, профилисање и биометријски надзор отварају нова питања у погледу заштите основних права и приватности, захтевајући додатне механизме за обезбеђење транспарентности, контроле и објашњивости алгоритама. Европски Акт о вештачкој интелигенцији уводи прецизније регулаторне инструменте, али његова примена ће тек показати домет у пракси, посебно у транснационалном контексту.

Случајеви анализирани у студијама случаја показују да су повреде података присутне како у јавном, тако и у приватном сектору, те да се неретко дешавају упркос постојању формалних механизама заштите. Посебно је значајна чињеница да европски правни поредак, кроз пресуде као што је Schrems II, показује тенденцију јачања контроле над међународним преносом података, што има директне последице по националне правне системе. Истовремено, примери као што је компанија Clearview AI указују на потребу за глобалним дијалогом и координисаном реакцијом надлежних органа на злоупотребу података у ери масовне примене вештачке интелигенције.

Унапређење система заштите података о личности у Републици Србији захтева целовит приступ који подразумева континуирано усклађивање домаћег правног оквира са стандардима Европске уније, уз истовремено јачање институционалних капацитета Повереника. Од кључне је важности и подизање нивоа свести и едукације, како руковалаца и обрађивача, тако и грађана, о њиховим правима и обавезама у области заштите података о личности. Поред тога, неопходно је развити прецизније правне механизме који ће регулисати обраду података употребом система заснованих на вештачкој интелигенцији, с обзиром на њихов растући утицај и потенцијалне ризике по основна права појединаца.

Изградња ефикасног система заштите података о личности у савременом дигиталном друштву захтева свеобухватан приступ који укључује предузимање превентивних мера, обезбеђење транспарентности обраде података, јасну одговорност свих актера и снажан механизам надзора на обрадом података о личности. Само такав приступ може допринети јачању поверења грађана у институције и обезбедити делотворну заштиту основних права у ери технолошке трансформације.

ЛИТЕРАТУРА

1. Андоновић Стефан, Прља Драган, *Основи права заштите података о личности*, Београд, 2020, Институт за упоредно право;
2. Андоновић Стефан, Лице за заштиту података о личности у правном систему Србије; у: Андоновић Стефан, Прља Драган, Дилигенски Андреј (ур.), *Заштита података о личности у Србији*, Београд, 2020, Институт за упоредно право, стр. 117-128;
3. Bogendorfer Rainer, Datenschutz-Grundverordnung, in: Knyrim Roland, (ed.), *Datenschutzrecht*, Vienna, 2016, Verlag Österreich, 172-174;
4. Дилигенски Андреј, Вредност података о личности; у: Андоновић Стефан, Прља Драган, Дилигенски Андреј (ур.), *Заштита података о личности у Србији*, Београд, 2020, Институт за упоредно право, стр. 19-32.
5. Дилигенски Андреј, Прља Драган, *Фејсбук, заштита података и судска пракса*, Београд, 2018, Институт за упоредно право;
6. Дилигенски Андреј, Прља Драган, Церовић Дражен, *Право заштите података ГДПР*, Београд, 2018, Институт за упоредно право;
7. Гасми Гордана, Прља Драган, Право на поштовање приватног живота и право на заштиту података о личности; у: Андоновић Стефан, Прља Драган, Дилигенски Андреј (ур.), *Заштита података о личности у Србији*, Београд, 2020, Институт за упоредно право, стр. 5-17;
8. Гасми Гордана, *Quo vadis EU?- Релевантни правни и институционални фактори*, Београд, 2016, Институт за упоредно право;
9. Hargittai Eszter, Marwick Alice, "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy, *International Journal of Communication*, Vol. 10, pp. 3737–3757;
10. Јовановић Зоран, Андоновић Стефан, Врсте информација и података у јавном праву Републике Србије; у: Андоновић Стефан, Прља Драган, Дилигенски Андреј (ур.), *Заштита података о личности у Србији*, Београд, 2020, Институт за упоредно право, стр. 33-46;
11. Krivokapić Đorđe, Krivokapić Danilo, Todorović Ivan, Komazec Stefan, Mapping Personal Data Flow and Regulatory Compliance in Serbian Public Institutions, *Management: Journal of Sustainable Business and Management Solutions in Emerging Economies*, no. 80, Vol. 21, pp. 1–10;
12. Лилић Стеван, Инспекцијска и друга овлашћења Повереника за заштиту података о личности; у: Андоновић Стефан, Прља Драган, Дилигенски Андреј (ур.), *Заштита података о личности у Србији*, Београд, 2020, Институт за упоредно право, стр. 105-116;
13. Lambert Paul, *The Data Protection Officer: Profession, Rules, and Role*, Boca Raton, 2017, CRC Press, Taylor & Francis Group;
14. Popović V. Dušan, The Pivotal Role of DPAs in Digital Privacy Protection: Assessment of the Serbian Protection Mechanism; in: Halmai Gábor, Bárd Petra (ed.), *Liberty and Security in Europe – LIVe 4*, Budapest, 2022, Centre for Social Sciences, Hungarian Academy of Sciences, 131–146.
15. Путник Ненад, Милошевић М. Младен, Цветковић Владимир, Рансомвер као претња безбедности – друштвени и кривичноправни аспекти, *Социолошки преглед,* бр. 1, Vol. 56, стр. 328-353;
16. Прља Драган, Гасми Гордана, Корać Вања, *Вештачка интелигенција у правном систему ЕУ*, Београд, 2021, Институт за упоредно право;

17. Прља Драган, Андоновић Стефан, Накнада штете код повреде личних података; у: Петровић Здравко, Чоловић Владимир (ур.), *Одговорност за штету, накнада штете и осигурање*, Београд-Ваљево, 2018, Институт за упоредно право, стр. 227-240;
18. Söderlund Kasia, Larsson Stefan, Enforcement Design Patterns in EU Law: An Analysis of the AI Act, *Digital Society*, no. 41, Vol. 3, 2024, pp. 1–21;
19. Zarrabi Fatemeh, Wagner Isabel, Boiten Eerke, Changes in Conducting Data Protection Risk Assessment: Before and After GDPR implementation, *Proceedings on Privacy Enhancing Technologies*, No. 4, Vol. 2023, pp. 185-209.
20. Wang Meng, Qin Yalin, Liu Jiaojiao, Li Weidong, Identifying Personal Physiological Data Risks to the Internet of Everything: the Case of Facial Data Breach Risks, *Humanities and Social Sciences Communications*, no. 216, Vol. 10, pp. 1-15.

Остала истраживачка грађа

1. Carlson Andrew, *Edward Snowden: Traitor or Hero*, (2022); преузето 3.4.2025. https://ethicsunwrapped.utexas.edu/case-study/edward-snowden-traitor-hero
2. Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, Judgment of 16 July 2020, ECLI:EU:C:2020:559, p. I-203.
3. Case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, Judgment of 1 October 2015, ECLI:EU:C:2015:639, p. I-66.
4. Директива ЕУ 2016/680 Европског парламента и Већа о заштити појединаца у вези с обрадом података о личности од стране надлежних органа у сврхе спречавања, истраге, откривања или гоњења учинилаца кривичних дела или извршавања кривичних санкција и о слободном кретању таквих података, *Службени лист ЕУ*, бр. L 119/89 од 4.5.2016. године.
5. Директива ЕУ 95/46/ЕЗ Европског парламента и Савета о заштити грађана у вези са обрадом података о личности и о слободном кретању таквих података, *Службени лист Европских заједница,* бр. L 281 од 23.11.1995. године.
6. European Data Protection Board, *The French SA fines Clearview AI EUR 20 million*, (2022); преузето 4.7.2025. https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en
7. European Data Protection Board, *Facial recognition: Italian SA fines Clearview AI EUR 20 million,* (2022); преузето 4.7.2025. https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en
8. European Data Protection Board. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1*, Brussels, 2019.
9. Извршна одлука Комисије (ЕУ) 2023/1795 од 10. јула 2023. године, у складу са Уредбом (ЕУ) 2016/679 Европског парламента и Савета, о адекватном нивоу заштите личних података у оквиру ЕУ–САД оквира за приватност података (EU–U.S. Data Privacy Framework), саопштено под бројем документа C(2023) 4745, *Службени лист ЕУ*, L 191, од 14.7.2023.
10. Кривични законик, *Службени гласник РС*, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 и 94/2024.
11. Милошевић М. Младен, *Одговорност правних лица за кривична дела*, (2012); преузето 25.6.2025. https://nardus.mpn.gov.rs/bitstream/handle/123456789/2601/Disertacija.pdf?sequence=4&isAllowed=y

12. Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника за информације од јавног значаја и заштиту података о личности, *Службени гласник РС*, бр. 45/2019.
13. Повереник за информације од јавног значаја и заштиту података о личности. *Извештај о раду за 2024. годину*, Београд, 2025.
14. Повереник за информације од јавног значаја и заштиту података о личности, *Повереник спровео поступак надзора у МУП, поводом сумњи на употребу технологије за препознавање лица (Facial Recognition Technology)*, (2022); преузето 1.7.2025. https://www.poverenik.rs/sr-yu/saopstenja/3730-повереник-спровео-поступак-надзора-у-муп,-поводом-сумњи-на-употребу-технологије-за-препознавање-лица-facial-recognition-technology.html
15. Повереник за информације од јавног значаја и заштиту података о личности. *Извештај о раду Повереника за информације од јавног значаја и заштиту података о личности за 2021. годину*, Београд, 2022.
16. Правилник о обрасцу и начину вођења евиденције лица за заштиту података о личности, *Службени гласник РС*, бр. 40/2019.
17. Повеља Европске Уније о основним правима, *Службени лист Европске уније,* бр. C 202 од 7.6.2016. године.
18. Радна група члана 29. *Смернице о лицима за заштиту података, 16/EN, WP 243 rev. 01*, Брисел, 2016.
19. Стратегија развоја вештачке интелигенције у Републици Србији за период 2025-2030. године, *Службени гласник РС,* бр. 5/2025.
20. Sharma Nitish, *Case Study: The WannaCry Ransomware Attack*, (2024); преузето 3.4.2025. https://medium.com/@nitishsharma9136/case-study-the-wannacry-ransomware-attack-c010789be119
21. Support4Partnership, *The fight in Serbia over Chinese-style surveillance (Part One)*, (2022); преузето 1.7.2025. https://support4partnership.org/en/news/the-fight-in-serbia-over-chinese-style-surveillance-part-one
22. Thielman Sam, Johnston Chris, *Major cyber attack disrupts internet service across Europe and US*, (2016); преузето 3.4.2025. https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service
23. Thompson Derek, *Google's CEO: 'The Laws Are Written by Lobbyists'*, (2010); преузето 3.4.2025. https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/
24. Уредба (ЕУ) 2024/1689 Европског парламента и Савета од 13. јуна 2024. о утврђивању усклађених правила о вештачкој интелигенцији и мењању Уредбе (ЕЗ) бр. 300/2008, (ЕУ) бр. 167/2013, (ЕУ) бр. 168/2013, (ЕУ) 2018/858, (ЕУ) 2018/1139 и (ЕУ) 2019/2144, као и Директиве 2014/90/ЕУ, (ЕУ) 2016/797 и (ЕУ) 2020/1828 (Акт о вештачкој интелигенцији), *Службени лист Европске уније,* бр. L 1689 од 12.7.2024. године.
25. Уредба (ЕУ) 2016/679 Европског парламента и већа од 27. априла 2016. о заштити појединаца у вези са обрадом личних података и о слободном кретању таквих података те о стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података), *Службени лист ЕУ*, бр. L 119/1 од дана 4.5.2016. године.
26. Закон о привредним друштвима, *Службени гласник РС*, бр. 6/2011, 99/2011, 83/2014 - др. закон, 5/2015, 44/2018, 95/2018, 91/2019, 109/2021 и 19/2025.
27. Закључак о усвајању етичких смерница за развој, примену и употребу поуздане и одговорне вештачке интелигенције, *Службени гласник РС,* бр. 23/2023.

28. Закон о облигационим односима, *Службени лист СФРЈ*, бр. 29/78, 39/85, 45/89 - одлука УСЈ и 57/89, *Службени лист СРЈ*, бр. 31/93, *Службени лист СЦГ*, бр. 1/2003 - Уставна повеља и *Службени гласник РС*, бр. 18/2020.
29. Закон о заштити података о личности, *Службени гласник РС*, бр. 87/18.
30. Закон о заштити података о личности, *Службени гласник РС*, бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012.
31. Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података, *Службени лист СРЈ - Међународни уговори, бр. 1/92, Службени лист СЦГ – Међународни уговори, бр. 11/2005 - др. закон и Службени гласник РС - Међународни уговори, бр. 98/2008 - др. закон и 12/2010*.
32. Закон о одговорности правних лица за кривична дела, *Службени гласник РС*, бр. 97/2008.
33. Закон о заштити података о личности, *Службени лист СРЈ*, бр. 24/98 и 26/98 - исправка.

Сажетак
Правни аспекти повреде података о личности у Републици Србији

У ери убрзаног развоја дигиталних технологија, питање заштите података о личности постаје један од најзначајнијих правних и друштвених изазова. Овај рад се бави анализом правних аспеката повреде података о личности у Републици Србији, усклађеношћу са прописима Европске уније, као и проблемима у примени самог закона у пракси. Акценат је стављен на све учесталије случајеве повреда података, уз осврт на механизме превенције и управљања инцидентима, као и утицај савремених технологија, пре свега вештачке интелигенције, на безбедност и приватност појединаца.

У раду се анализира нормативни оквир заштите података у Републици Србији и Европској унији, укључујући Општу уредбу о заштити података, Полицијску директиву и Акт о вештачкој интелигенцији ЕУ. Посебна пажња посвећена је Закону о заштити података о личности из 2018. године, његовим недостацима, као и предстојећим изменама у светлу нове Стратегије и Акционог плана. Такође, у раду је обрађена проблематика повреде података о личности кроз теоријску и практичну призму, па су стога анализирани узроци инцидената, правне последице, као и извештај Повереника за 2024. годину.

Посебан део рада посвећен је превентивним и репресивним механизмима: процени утицаја, именовању лица за заштиту података, евиденцији радњи обраде, техничким и организационим мерама заштите, као и улози Повереника. У раду су обрађене и

последице повреде података, односно питања одговорности за повреде података о личности. Посебно је анализиран ризик од повреда у контексту примене вештачке интелигенције: профилисање, биометријски надзор и нетранспарентност алгоритама. Кроз студије случаја (МУП Србије, Ерсте банка, Schrems II, Clearview AI), указано је на конкретне повреде у јавном и приватном сектору.

На крају рада закључује се да Република Србија поседује нормативне и институционалне капацитете за ефикасну заштиту података о личности, али да је потребно њихово доследније спровођење у пракси, јачање надзорних тела и увођење строжих регулаторних механизама за обраду података путем вештачке интелигенције. Унапређење свести грађана, едукација и доследна примена прописа представљају кључне кораке ка изградњи правно сигурнијег система заштите података.

Кључне речи: заштита података о личности, повреда података, правни оквир, Повереник за информације од јавног значаја и заштиту података о личности, ГДПР, вештачка интелигенција

Abstract

Legal Aspects of Personal Data Breaches in the Republic of Serbia

In an era of rapid digital technology development, the issue of personal data protection has become one of the most significant legal and societal challenges. This paper analyzes the legal aspects of personal data breaches in the Republic of Serbia, the alignment with European Union regulations, as well as the practical issues in the implementation of the law. The focus is placed on the increasingly frequent cases of data breaches, with a review of prevention and incident management mechanisms, as well as the impact of modern technologies, particularly artificial intelligence, on individual security and privacy.

The paper examines the normative framework for data protection in the Republic of Serbia and the European Union, including the General Data Protection Regulation (GDPR), the Police Directive, and the EU Artificial Intelligence Act (AI Act). Special attention is given to the 2018 Law on Personal Data Protection in Serbia, its shortcomings, and the forthcoming amendments in light of the new Strategy and Action Plan. Furthermore, the issue of personal data breaches

is addressed from both theoretical and practical perspectives, analyzing the causes of incidents, legal consequences, and the 2024 Report of the Commissioner.

A separate part of the paper is dedicated to preventive and repressive mechanisms: data protection impact assessments, the designation of data protection officers, records of processing activities, technical and organizational security measures, and the role of the Commissioner. The consequences of data breaches are also discussed, particularly questions of liability for personal data violations. Special emphasis is placed on the risk of breaches in the context of artificial intelligence applications: profiling, biometric surveillance, and algorithmic opacity. Through case studies (Ministry of Internal Affairs of Serbia, Erste Bank, Schrems II, Clearview AI), the paper highlights specific breaches in both the public and private sectors.

The paper concludes that the Republic of Serbia possesses the normative and institutional capacities for effective personal data protection, but emphasizes the need for more consistent enforcement, strengthening of supervisory bodies, and the introduction of stricter regulatory mechanisms for data processing via artificial intelligence. Raising public awareness, education, and consistent application of regulations are identified as key steps toward building a more legally secure data protection system.

Keywords: personal data protection, data breach, legal framework, Commissioner for Information of Public Importance and Personal Data Protection, GDPR, artificial intelligence

Биографија студента

Наташа Вуковић је рођена 1994. године у Градишци, Република Српска. Основне академске студије завршила је 2020. године на Правном факултету Универзитета у Бањој Луци. Године 2023. успешно је окончала програм стручног усавршавања на Факултету безбедности Универзитета у Београду и стекла звање менаџера заштите података о личности. Школске 2023/2024. године уписала је мастер академске студије на Правном факултету Универзитета у Нишу, смер право и информационе технологије.

Досадашње радно искуство стекла је у адвокатским канцеларијама у Бањој Луци и Београду, као и у привредном сектору, пружајући правне услуге у области информационих технологија.

Професионална интересовања усмерена су ка пружању правне подршке привредним друштвима из сектора информационих технологија, с фокусом на унапређење правне сигурности и ефикасности пословања. Посебно је заинтересована за правне аспекте заштите података о личности, вештачке интелигенције и уопштено за примену права у дигиталном окружењу.

Приправнички стаж у Републици Србији завршила је у адвокатској канцеларији у Београду и тренутно се припрема за полагање правосудног испита.

Говори енглески језик.

ИЗЈАВА О ИСТОВЕТНОСТИ
ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: Наташа Вуковић

Наслов мастер рада: Правни аспекти повреде података о личности у Републици Србији

Ментор: Проф. др Дејан Вучетић

Изјављујем да је електронски облик мастер рада у pdf формату истоветан штампаном облику, који сам предао/ла Правном факултету Универзитета у Нишу.

У Нишу, 15. 8. 2025.

Потпис аутора

Наташа Вуковић

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом Правни аспекти повреде података о личности у Републици Србији
пријављен и одбрањен на Правном факултету Универзитета у Нишу:
• резултат сопственог истраживачког рада;
• да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;
• да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

Дозвољавам да се овај мастер рад чува у библиотеци и објави на сајту Правног факултета Универзитета у Нишу, са подацима о датуму одбране и комисији пред којом је рад брањен.

Аутор мастер рада: Наташа Вуковић

У Нишу, 15.8.2025.

Потпис аутора

Наташа Вуковић