

УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ



Посебни подаци о личности

(мастер рад)

Студент:

Милица Пауновић M004/24-ИТ

Ментор:

Проф. др Милош Прица

Ниш, 2026.

САДРЖАЈ

УВОД	3
I ПОЈАМ И ПРАВНА ПРИРОДА ПОДАТАКА О ЛИЧНОСТИ.....	6
1.1 <i>Историјски развој концепта права личности</i>	<i>10</i>
1.2 <i>Теоријски оквири и доктринарна схватања</i>	<i>16</i>
1.3 <i>Права личности у уставноправном систему Републике Србије.....</i>	<i>22</i>
II ПОЈАМ И ЗНАЧАЈ ПОСЕБНИХ ПОДАТАКА О ЛИЧНОСТИ	28
2.1 <i>Дефиниција и класификација посебних података о личности</i>	<i>30</i>
2.2 <i>Посебни подаци и њихова улога у заштити приватности</i>	<i>38</i>
2.3 <i>Однос између општих и посебних података о личности</i>	<i>42</i>
III НОРМАТИВНИ ОКВИР У РЕПУБЛИЦИ СРБИЈИ	44
3.1 <i>Уставна заштита права личности</i>	<i>45</i>
3.2 <i>Закон о заштити података о личности</i>	<i>52</i>
3.3 <i>Улога Повереника за информације од јавног значаја и заштиту података о личности.....</i>	<i>57</i>
IV ЕВРОПСКИ ПРАВНИ СТАНДАРДИ	63
4.1 <i>Општа уредба о заштити података (GDPR).....</i>	<i>63</i>
4.2 <i>Европска конвенција о људским правима и релевантна пракса Европског суда за људска права (ЕСЉП)</i>	<i>72</i>
4.3 <i>Хармонизација српског законодавства са европским стандардима</i>	<i>79</i>
V ИЗАЗОВИ И ПРАКТИЧНИ ПРОБЛЕМИ У ПРИМЕНИ.....	83
5.1 <i>Технолошки развој и дигитализација као изазов</i>	<i>83</i>
5.2 <i>Злоупотреба података у пракси</i>	<i>88</i>
5.3 <i>Баланс између јавног интереса и права личности</i>	<i>92</i>
VI КОМПАРАТИВНА АНАЛИЗА.....	94
6.1 <i>Упоредноправни преглед – Немачка, Француска и Велика Британија ...</i>	<i>95</i>
6.1.1 <i>Немачка.....</i>	<i>95</i>

6.1.2 Француска	98
6.1.3 Велика Британија.....	100
6.1.4 Компаративно сагледавање три модела и могућности примене у Србији	104
6.2 Практична искуства у примени GDPR	106
6.3 Могућност примене добрих пракси у Србији	108
ЗАКЉУЧАК	111
САЖЕТАК.....	114
SUMMARY.....	115
СПИСАК КОРИШЋЕНЕ ЛИТЕРАТУРЕ.....	116
БИОГРАФИЈА.....	120

УВОД

Појам података о личности представља једну од темељних категорија савременог права заштите личности, јер се управо кроз њега успоставља веза између човека као носиоца права и информација које се односе на њега. Развој овог појма није био изолован од ширих промена у схватању личности, приватности и људског достојанства. Напротив, његово савремено значење представља резултат постепеног преобликовања правне мисли: од схватања личности као претежно приватне сфере појединца, преко признавања права на приватност, до савременог разумевања информационе аутономије и права појединца да има одређену контролу над информацијама које се о њему прикупљају, чувају, користе и размењују.

Историјски посматрано, заштита личности најпре се развијала кроз признавање права која су штитила физички и морални интегритет човека, његову част, углед, достојанство и приватни живот. Са развојем модерног друштва, а нарочито са појачањем процеса технолошке обраде информација, постало је јасно да традиционални облици заштите приватности нису довољни за све ситуације у којима се личност може угрозити. Чињеница да се информације о једном лицу могу систематски прикупљати, повезивати, анализирати и употребљавати у различите сврхе довела је до потребе да се правна заштита прошири и на саму информациону сферу личности. У том процесу посебан значај добија идеја да човек не треба да буде заштићен само од непосредног и физичког задирања у своју приватност, већ и од неконтролисаног располагања информацијама које га описују или се са њим могу повезати.

Управо се на том месту формира савремени концепт података о личности. Они више нису само технички запис одређене чињенице, већ представљају информациони аспект личности који може имати непосредне последице по њен положај, права, слободе и достојанство. Посебан значај у том контексту имају посебне врсте података о личности, чија природа и садржина могу носити повећан ризик за права и слободе физичких лица. Њихова заштита зато не представља само питање формалне класификације података, већ

питање успостављања одговарајуће равнотеже између потребе за обрадом података и заштите приватности, достојанства и аутономије личности.

Предмет овог рада јесте анализа посебних категорија података о личности, њихове правне природе, места у систему заштите података о личности и посебних услова под којима се могу обрађивати. Посебна пажња посвећена је нормативном оквиру Републике Србије, односу општег режима заштите података и посебног режима који се примењује на осетљивије категорије података, као и европским и међународним стандардима који су утицали на развој савременог система заштите. У том смислу, питање посебних података не посматра се изоловано, већ у ширем контексту права на приватност, информационе аутономије и заштите основних права личности.

Истраживање је усмерено и на испитивање односа између нормативне уређености и стварне делотворности заштите. Иако је доношењем Закона о заштити података о личности из 2018. године Република Србија направила значајан корак ка приближавању свог правног система савременим европским стандардима, сама формална усклађеност правних норми није довољна за постизање потпуне заштите. Степен остваривања права лица чији се подаци обрађују зависи и од начина примене прописа, усклађености секторских правила, институционалних и кадровских капацитета, техничких и организационих мера, као и од способности правног система да одговори на нове облике обраде података. Посебно значајним показује се питање здравствених, генетичких и биометријских података, као и ризика који настају њиховим повезивањем са другим категоријама података, профилисањем и употребом у нове сврхе.

Основна хипотеза рада полази од претпоставке да је нормативни оквир Републике Србије у области заштите посебних података о личности у значајној мери приближен савременим европским стандардима, али да између формалне нормативне усклађености и стварне, делотворне примене и даље постоји простор за унапређивање. Проблем се, према томе, не огледа нужно у потпуном недостатку правних инструмената, већ пре свега у њиховој неуједначеној примени, недовољној усклађености појединих секторских прописа, институционалним и кадровским ограничењима и потреби да се постојећи механизми прилагоде новим облицима обраде података. Отуда се хармонизација домаћег права са

европским стандардима не може схватити као једнократан процес преузимања нормативних решења, већ као континуирано усавршавање правних, институционалних и практичних механизма заштите.

У том контексту, значајно место у раду заузимају и институционална и судска заштита. Делотворна заштита посебних података о личности не зависи само од садржине материјалноправних правила, већ и од способности надзорних и судских органа да та правила примене у конкретним ситуацијама. Посебан значај има улога Повереника за информације од јавног значаја и заштиту података о личности, како у погледу надзора и корективних овлашћења, тако и у погледу превентивног деловања, стручних упутстава и развоја праксе. Истовремено, развој домаће судске праксе представља важан предуслов за уједначавање стандарда и обезбеђивање делотворне заштите, нарочито у областима у којима се јављају нови облици ризика, као што су биометријска идентификација, видео-надзор, електронске комуникације, профилисање и аутоматизовано доношење одлука.

Посебан допринос истраживању пружа упоредноправна анализа Немачке, Француске и Велике Британије. Циљ овог поређења није утврђивање који правни систем садржи „боље“ или „строже“ решење, већ идентификовање функционално упоредивих механизма и добрих пракси које би, уз одговарајуће прилагођавање домаћем правном и институционалном контексту, могле допринети даљем развоју система заштите у Републици Србији. Немачко искуство посебно указује на значај информационог самоопредељења и начела пропорционалности, француско на значај активног и превентивног деловања надзорног органа, док британско искуство указује на изазове које савремене технологије, нарочито у области биометријске обраде, постављају пред традиционалне механизме заштите. Упоредно право се зато у овом раду не користи као основ за механичко преузимање туђих решења, већ као средство за критичко сагледавање домаћег система и могућих праваца његовог унапређивања.

Методолошки, истраживање се заснива на међусобно повезаној примени нормативне, компаративне, историјскоправне, аналитичко-синтетичке и емпиријске методе. Нормативна метода примењена је у анализи Устава Републике Србије, Закона о заштити података о личности, европских и међународних правних инструмената, као и

релевантних правних правила која уређују обраду посебних врста података. Компаративна метода омогућила је сагледавање решења Немачке, Француске и Велике Британије, док је историјскоправна метода коришћена ради праћења развоја права на приватност и заштите података. Аналитичко-синтетичким приступом повезани су појединачни правни институти, нормативна решења, судска и институционална пракса, док је емпиријска компонента остварена кроз анализу конкретних случајева и стварне праксе домаћих и европских институција и судова. Таква методолошка поставка омогућава да се предмет истраживања не сагледа само кроз текст правних норми, већ и кроз њихов историјски развој, практичну примену и место у различитим правним системима.

Коначно, истраживање полази од схватања да се квалитет система заштите посебних података о личности не може мерити искључиво бројем усвојених правних правила, већ њиховом способношћу да у стварним животним ситуацијама обезбеде делотворну заштиту права и слобода појединца. Даљи развој домаћег система зато подразумева не само наставак хармонизације са европским стандардима, већ и усклађивање секторских прописа, јачање институционалних и стручних капацитета, развој превентивних механизма, унапређење техничких и организационих мера безбедности и постепено формирање уједначене судске праксе. Крајњи циљ таквог приступа није формално приближавање домаћег законодавства европским моделима, већ успостављање система у којем су приватност, достојанство, информациона аутономија и друга права лица чији се подаци обрађују стварно, делотворно и континуирано заштићени.

I ПОЈАМ И ПРАВНА ПРИРОДА ПОДАТАКА О ЛИЧНОСТИ

Теоријска схватања права личности доприносе разумевању овакве природе података. Права личности полазе од идеје да постоје добра која су нераскидиво повезана са самом личношћу човека и која, управо због те повезаности, заслужују посебну правну заштиту. У ту групу традиционално се убрајају живот, телесни интегритет, част, углед, приватност, достојанство и други аспекти личне сфере¹. Савремени развој информационог

¹ И. Симовић, М. Лазић, „Грађанско-правна заштита права личности“, *Зборник радова Правног факултета у Нишу*, бр. 68, 2014;

друштва овом корпусу придружује и информациони аспект личности², јер подаци о појединцу могу постати средство помоћу којег се његов живот, идентитет, навике, односи и карактеристике представљају другима.

У том смислу, право на заштиту података о личности не треба посматрати као потпуно одвојено од права на приватност, али ни као његов прост синоним. Приватност првенствено штити простор личне сфере од неовлашћеног уплитања, док заштита података о личности обухвата шири круг питања која се односе на начин поступања са информацијама о појединцу. Обрада података може бити правно релевантна и онда када не доводи до традиционално схваћеног „уласка у приватност“. Само прикупљање, чување, повезивање или откривање одређених података може створити ризик за права и слободе појединца, нарочито када се врши систематски, у великом обиму или употребом савремених технологија.

Из овога произлази једна од суштинских карактеристика података о личности: њихова правна релевантност не произлази само из садржине податка, већ и из односа тог податка према одређеном физичком лицу и начина на који се њиме поступа. Податак који сам по себи изгледа безазлено може, у комбинацији са другим подацима, открити знатно више о личности. Адреса, подаци о кретању, подаци о куповини, интернет активности или технички идентификатори, посматрани појединачно, могу имати ограничену информативну вредност, али њиховим повезивањем може настати веома детаљна слика о навикама, интересовањима и понашању појединца. На тај начин, правни значај података произлази и из могућности њиховог повезивања и даље обраде.

Управо је ова динамичност информационе сфере допринела развоју концепта информационе аутономије. Њена суштина није у апсолутном праву појединца да сакрије све информације о себи, већ у признавању његовог легитимног интереса да зна, у одређеној мери утиче и има правну заштиту у погледу начина на који се информације о њему користе. Информациона аутономија зато представља важну теоријску основу

² Hüseyin Can Aksoy, „The Right to Personality and Its Different Manifestations as the Core of Personal Data“, *Ankara Law Review*, Vol. 5, No. 2, 2008, стр. 235–249.

савременог права заштите података о личности³. Она повезује приватност, достојанство и слободно развијање личности са потребом да обрада података буде ограничена правом, сврхом и принципом сразмерности.

Уставноправна димензија овог питања у Републици Србији посебно је значајна. Устав Републике Србије у члану 42. изричито гарантује заштиту података о личности и прописује да је забрањена и кажњива употреба података о личности изван сврхе за коју су прикупљени, као и да свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом. На тај начин заштита података о личности добија самосталну уставноправну димензију и више се не може свести само на један од аспеката заштите приватности.

Уставна гаранција мора се, међутим, посматрати у ширем систему заштите права личности. Достојанство личности, неповредивост физичког и психичког интегритета, право на приватност и породични живот, слобода мисли и уверења, као и друга уставом заштићена права, представљају међусобно повезане елементе правног положаја појединца. Подаци о личности могу истовремено бити повезани са различитим од ових права, због чега њихова заштита има вишедимензионални карактер.

Посебно место у том систему има Закон о заштити података о личности, којим се детаљније уређују права физичких лица у вези са обрадом њихових података, обавезе руковалаца и обрађивача, начела обраде, правни основи, мере заштите, надзор и правна средства. Савремени српски нормативни оквир у значајној мери је обликован под утицајем европских стандарда, пре свега Опште уредбе о заштити података. Тиме је појам података о личности постављен у средиште ширег система правила чија сврха није само спречавање злоупотребе већ и обезбеђивање законите, поштене, транспарентне и сразмерне обраде.

Из правне природе података о личности произлази и њихова двострука особеност. С једне стране, податак је информација која може бити предмет техничке обраде, чувања, преноса и анализе. С друге стране, та информација је правно повезана са конкретном

³ F. Thouvenin, "Informational Self-Determination: A Convincing Rationale for Data Protection Law?", *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 12, No. 4, 2021, стр. 246–250.

личношћу и може утицати на њен положај⁴. Управо због тога податак о личности не може бити посматран искључиво као неутрална информација или као обичан ресурс којим се слободно располаже. Његова употреба мора бити подвргнута правним ограничењима која проистичу из права личности и основних начела заштите података.

Ова карактеристика постаје још израженија код посебних врста података о личности. Подаци који откривају здравствено стање, генетске карактеристике, биометријске особине, расно или етничко порекло, политичка мишљења, верска или филозофска уверења, чланство у синдикату, сексуални живот или сексуалну оријентацију могу дубље задрети у најинтимније сфере човековог живота и створити повећан ризик од дискриминације, стигматизације, злоупотребе или других облика повреде права. Због тога њихова правна заштита почива на строжем режиму и представља посебан израз општег принципа да степен правне заштите треба да одговара степену ризика који обрада одређене категорије података носи⁵.

Посматрано у целини, појам података о личности налази се на пресеку више правних вредности. Он повезује право на приватност са достојанством, аутономијом, слободом личности и забраном дискриминације. Истовремено, он повезује индивидуални интерес појединца са легитимним интересима других лица, привредних субјеката и јавних власти да податке обрађују када за то постоји одговарајући правни основ и оправдана сврха. Зато заштита података није заснована на апсолутном искључењу других из информационе сфере појединца, већ на успостављању правних граница унутар којих је њихова обрада допуштена.

Правна природа података о личности, према томе, не може се исцрпети у њиховом формалном одређењу као информација која се односи на физичко лице. Њихов суштински значај произлази из чињенице да представљају информациони одраз личности и да, зависно од начина употребе, могу утицати на њену слободу, достојанство, приватност и положај у друштву. Савремено право зато постепено напушта схватање према којем је довољно реаговати тек након што је приватност непосредно повређена и све више

⁴ Андоновић, С. и Прља, Д. Основи права заштите података о личности, Београд: Институт за упоредно право, 2020, стр. 9-10;

⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council, Rec. 51.

инсистира на превентивној заштити, контроли сврхе обраде, минимизацији података, ограничењу приступа, времену чувања и одговарајућим техничким и организационим мерама.⁶

Најзад, подаци о личности представљају једну од најзначајнијих правних категорија савременог информационог друштва управо зато што се у њима сусрећу информација и личност. Њихова правна заштита није само питање контроле над подацима, већ и питање граница утицаја других лица и институција на појединца. Од историјског развоја права личности, преко теоријског концепта информационе аутономије, до уставне гаранције заштите података о личности у Републици Србији, постепено се обликује једна иста правна идеја: човек не престаје бити носилац достојанства и аутономије онда када се о њему створе дигитални записи. Напротив, што је могућност прикупљања, повезивања и анализе података већа, то постаје значајнија обавеза права да одреди границе унутар којих информације о човеку могу постати предмет обраде, а да човек при том не постане само предмет те обраде.

1.1 Историјски развој концепта права личности

Права личности представљају једну од значајних категорија савременог приватног права, а њихов развој представља дуготрајан процес постепеног издвајања и правне заштите добара непосредно повезаних са личношћу човека. Међу њима се издвајају живот, телесни и психички интегритет, част, углед, достојанство, приватност, име, лик и идентитет.

Историјски посматрано, развој права личности може се разумети као процес постепеног померања тежишта правне заштите са имовине и формалног статуса лица ка заштити човека као личности. У најстаријим правним системима човек није био посматран као универзални носилац једнаких права у данашњем смислу. Обим његове правне заштите често је зависио од друштвеног статуса, пола, припадности одређеној заједници или слободног односно робовског положаја. Ипак, још у античком праву могу се уочити институти који су представљали претече савремене заштите појединих личних добара.

⁶ Андоновић, С. и Прља, Д. Основи права заштите података о личности, Београд: Институт за упоредно право, 2020, стр. 66-73, 127.

Посебан значај у том погледу има римско право. Већ у римском праву постојали су механизми заштите појединих личних добара. Значајан институт била је *actio iniuriarum*⁷, тужба која је служила за заштиту од противправних напада на личност, нарочито на част и достојанство. Њен значај за каснији развој права личности огледа се у томе што је омогућавала правну реакцију не само на материјалну штету, већ и на повреде нематеријалних интереса човека. Међутим, положај појединца у римском праву битно се разликовао од положаја човека у савременом правном поретку. Правна заштита није била универзална, а статус појединца имао је изузетно велики значај. Због тога се не може говорити о постојању права личности у данашњем смислу, већ пре о постојању појединих правних механизма који су касније постали један од темеља за њихов развој.

После пропасти Западног римског царства долази до значајних промена у европским правним системима. У средњем веку правни положај појединца био је снажно условљен феудалним друштвеним поретком, сталешком припадношћу и религијским схватањима. Иако у том периоду није постојала јединствена доктрина права личности, развијале су се идеје које су постепено допринеле схватању човека као носиоца одређених природних и неотуђивих добара.

Хришћанска мисао имала је значајну улогу у обликовању идеје о достојанству човека⁸. Схватање човека као бића које поседује урођену вредност представљало је важну идејну основу за каснији развој концепта људских права. Паралелно са тим, развој канонског права и универзитетске правне науке допринео је очувању и поновном проучавању римскоправних института.

Посебан значај има развој природноправне школе, нарочито од XVII века. Природноправни мислиоци све више полазе од идеје да одређена права припадају човеку самим тим што је човек, а не зато што му их држава додељује⁹. Ова промена имала је далекосежне последице. Појединац се постепено издваја као самосталан правни и политички субјект, а државна власт се све више посматра као власт која мора бити ограничена одређеним основним правима појединца.

⁷ I. Jaramaz-Reskušić, „Iniuria in pre-classical Roman law: concept and protection“, *Zbornik Pravnog fakulteta u Zagrebu*, Vol. 61, No. 2, 2011, стр. 545–571;

⁸ Sigrid Müller, „Concepts and Dimensions of Human Dignity in the Christian Tradition“, *Interdisciplinary Journal for Religion and Transformation in Contemporary Society*, Vol. 6, No. 1, 2020, стр. 24–25.

⁹ Thomas Mautner, „Natural Law and Natural Rights“, у: Peter R. Anstey (ed.), *The Oxford Handbook of British Philosophy in the Seventeenth Century*, Oxford University Press, 2013, стр. 472–500;

XVIII век представља једну од кључних етапа у развоју савременог концепта права личности. Просветитељска филозофија у средиште правног и политичког поретка поставља појединца, његову слободу и достојанство. Идеја да су људи рођени слободни и једнаки, као и захтев за ограничењем државне власти, постали су основни елементи новог схватања односа између појединца и државе¹⁰.

Америчка и Француска револуција имале су посебан значај за нормативно обликовање ових идеја. Декларација независности Сједињених Америчких Држава из 1776. године и Декларација о правима човека и грађанина из 1789. године представљају важне историјске документе у процесу конституционализације индивидуалних права¹¹. Иако ови документи нису садржали савремену систематизацију права личности, они су поставили темељ за њихов даљи развој кроз признавање слободе, једнакости и основних права појединца.

На пољу приватног права посебно је значајна француска кодификација. Француски Грађански законик из 1804. године није садржао систематизовану категорију права личности, а његов концептуални центар представљала су пре свега имовинска права. Ипак, општа правила деликтне одговорности омогућила су развој судске заштите и у случајевима повреде нематеријалних добара¹². Према истраживањима историје француског права, концепт заштите личности као посебна правна тема нарочито се развија током друге половине XIX века.

У том процесу значајну улогу имала је судска пракса. Један од познатијих примера представља случај *Rachel*¹³ из 1858. године, који се у француској правној литератури често наводи као значајан моменат у развоју права на сопствени лик. Суд је у конкретном случају пружио заштиту од неовлашћеног приказивања лика познате глумице на самрти, чиме је допринео развоју схватања да лик човека може представљати самостално заштићено лично добро.

¹⁰ Christoph Schmitt-Maaß, „‘Lumen Supernaturale’ vs ‘Lumen Naturale’: Human Rights and Their Religious Implications in Natural Law in the Early Enlightenment (Pufendorf–Thomasius–Wolff)“, *German Life and Letters*, vol. 78, br. 1, 2025, стр. 16–17;

¹¹ Yvon Seren, „L'exemple américain dans les institutions issues de la Révolution française ; les déclarations américaines et la déclaration française des Droits de l'Homme et du Citoyen de 1789“, *Annales de Bretagne et des pays de l'Ouest*, t. 84, br. 3, 1977, стр. 283.

¹² Code civil des Français, 1804, art. 1382;

¹³ Jeanne Gillet, *Privacy and Online Surveillance: International Legal Challenges*, PhD thesis, School of Law, University of Glasgow, 2019, стр. 34–35;

XIX век представља период у коме долази до постепеног издвајања права личности као посебне правне категорије. Индустријализација, развој масовних медија, урбанизација и промене у друштвеним односима довели су до појаве нових облика угрожавања појединца. Истовремено, развој грађанског друштва и либералне политичке мисли допринели су јачању идеје индивидуалне аутономије.

У европским правним системима развијали су се различити приступи. Француско право је путем општих правила грађанске одговорности омогућавало заштиту нематеријалних интереса, док је немачка правна традиција дуго била усмерена на систематизацију посебних, конкретно одређених права. У Немачкој је заштита имена, лика и других аспеката личности постепено добијала нормативни и судски облик. С

Немачки Грађански законик (BGB), који је ступио на снагу 1900. године, садржао је поједине норме релевантне за заштиту личности, укључујући заштиту имена¹⁴. Касније је значајну улогу имао и посебан пропис - Закон о ауторском праву на делима визуелних уметности из 1907. године, који је регулисао и питање употребе лика¹⁵. Немачка судска пракса је током XX века постепено изградила шири концепт општег права личности.

Посебну етапу у историјском развоју права личности представља развој права на приватност. Његово савремено правно обликовање у Сједињеним Америчким Државама обично се повезује са радом Семјуела Ворена и Луиса Брендајса, који су 1890. године објавили познати чланак „The Right to Privacy“¹⁶. У њему су указали на потребу правне заштите појединца од неовлашћеног мешања у његов приватни живот, посебно у условима развоја штампе и нових технологија.

Развој масовних медија показао је да класична заштита имовине није довољна за заштиту личности. Фотографија, штампа и касније радио, телевизија и други облици масовне комуникације створили су могућност да се информације о приватном животу појединца шире великом броју људи без његове сагласности. На тај начин право је било принуђено да одговори на нове облике угрожавања личности.

¹⁴ Bürgerliches Gesetzbuch (BGB), 1900, § 12.

¹⁵ Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KUG), 1907, §§ 22–23;

¹⁶ Samuel D. Warren, Louis D. Brandeis, „The Right to Privacy“, *Harvard Law Review*, vol. 4, br. 5, 1890, стр. 193–195;

У америчком праву се временом развијају различити облици заштите приватности, као и право на контролу комерцијалног коришћења одређених аспеката личности, што се у литератури повезује са развојем тзв. „right of publicity“. Овај институт омогућава заштиту комерцијалне вредности идентитета појединца, нарочито његовог имена, лика и гласа. Његов развој посебно је значајан у контексту познатих личности, чији лични атрибути могу имати изражену комерцијалну вредност¹⁷.

XX век донео је даљу афирмацију права личности, а нарочито након Другог светског рата. Масовна кршења основних људских права током рата показала су да заштита личности не може бити искључиво питање унутрашњег права државе. Потреба за међународним механизмима заштите довела је до развоја међународног система људских права. Универзална декларација о људским правима из 1948. године представља један од кључних докумената у овом процесу. Након ње усвојени су бројни међународни уговори којима се утврђују стандарди заштите живота, слободе, достојанства, приватности и других основних права човека.

Посебан значај за европски правни простор има Европска конвенција за заштиту људских права и основних слобода, отворена за потписивање у Риму 4. новембра 1950. године, а која је ступила на снагу 1953. године. За развој права личности посебно је значајан члан 8. Европске конвенције, којим се гарантује право на поштовање приватног и породичног живота, дома и преписке¹⁸. Практична примена ове одредбе кроз праксу Европског суда за људска права довела је до значајног проширења разумевања приватног живота.

Развој заштите личности у српском правном систему треба посматрати у ширем контексту развоја грађанског и уставног права. Уставни развој Србије током XIX века постепено је доводио до признавања и гарантовања различитих права и слобода појединца. Историјски извори указују да су гаранције људских права биле присутне већ у Сретењском уставу из 1835. године¹⁹.

Каснији развој југословенског правног система значајан је за обликовање савремене грађанскоправне заштите личности. Посебно место има Закон о облигационим односима

¹⁷ Eric E. Johnson, „Disentangling the Right of Publicity“, *Northwestern University Law Review*, vol. 111, br. 4, 2017, стр. 891–962.

¹⁸ Европска конвенција за заштиту људских права и основних слобода, 1950, чл. 8;

¹⁹ Марковић, Р. „Сретењски устав – The Serbian ‘Sretenje’ Constitution“, *Анали Правног факултета у Београду*, год. 33, бр. 2, 1985, стр. 149–160;

из 1978. године, који је у области вануговорне одговорности поставио важне основе за заштиту нематеријалних добара. Закон о облигационим односима садржи опште механизме заштите личности. Према члану 157, свако има право да захтева престанак радње којом се повређује интегритет људске личности, лични и породични живот и друга права његове личности. Поред тога, чланови 199. и 200. предвиђају различите облике сатисфакције и правичну новчану накнаду за нематеријалну штету у случајевима које закон предвиђа.²⁰

Савремени уставни оквир Републике Србије додатно је ојачао заштиту личности. Устав Републике Србије из 2006. године у члану 23. изричито гарантује неприкосновеност људског достојанства и право на слободан развој личности. Члан 25. штити физички и психички интегритет. Посебно је значајан члан 42. Устава, којим се гарантује заштита података о личности. Ова гаранција показује како се традиционални концепт права личности прилагођава савременим условима у којима информације о појединцу могу бити прикупљане, обрађиване, чуване и преношене у великим количинама. Право на заштиту података тако постаје један од важних савремених аспеката заштите личности.²¹

Савремена технологија додатно је проширила подручје потенцијалних повреда. Дигитализација, друштвене мреже, биометријски подаци, системи аутоматизоване обраде података и вештачка интелигенција постављају нова питања у вези са заштитом личности. Податак о личности више није само традиционални податак попут имена или адресе, већ може обухватати велики број информација које омогућавају идентификацију или профилисање појединца. Због тога савремена права личности имају динамичан карактер. Њихов развој није завршен, већ се непрекидно прилагођава променама у друштву и технологији.

На основу свега наведеног, може се закључити да је историјски развој концепта права личности истовремено и историја постепеног јачања положаја појединца у правном поретку. Од правне заштите појединачних личних добара дошло се до схватања личности као јединствене вредности која ужива правну заштиту у различитим областима права. Тај процес и даље траје, јер се са појавом нових технологија и нових облика комуникације

²⁰ 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, чл. 157, 199. и 200.

²¹ Устав Републике Србије, „Службени гласник РС“, бр. 98/2006, чл. 23, 25 и 42.

појављују и нови изазови за очување човековог достојанства, приватности, идентитета и аутономије.

1.2 Теоријски оквири и доктринарна схватања

Потпуније разумевање института посебних података о личности претпоставља претходно разматрање његових теоријских и доктринарних основа. Иако се посебни подаци о личности у позитивном праву појављују као нормативно дефинисана категорија података која подлеже посебном режиму обраде, њихова правна природа и разлози због којих им се пружа појачана заштита не могу се у потпуности објаснити искључиво анализом законских одредаба. Напротив, њихово место у савременом правном систему потребно је сагледати у контексту ширег развоја права личности, права на приватност, људског достојанства, аутономије појединца и права на информационо самоодређење.

Посебни подаци о личности представљају један од најзначајнијих примера трансформације традиционалног концепта заштите личности под утицајем развоја информационог друштва. Док је класична правна теорија права личности била усмерена пре свега на заштиту живота, телесног и психичког интегритета, части, угледа, имена, лика и приватног живота²², савремени правни поредак све већу пажњу посвећује информационом аспект личности. Човекова личност више се не испољава само кроз физичко постојање и непосредне друштвене односе, већ и кроз огроман број информација које се о њему прикупљају, чувају, повезују, анализирају и користе.

Та промена довела је до постепеног напуштања схватања да је заштита приватности довољна сама по себи. Уместо тога, развија се сложенији концепт правне заштите који обухвата не само право појединца да одређене информације задржи ван домашаја других лица, већ и његово право да буде обавештен о томе које се информације о њему прикупљају, у коју сврху се користе, ко њима располаже и под којим условима се могу даље обрађивати. Овај развој има посебан значај када је реч о посебним подацима о

²² Симоновић, И., Лазић, М., „Грађанскоправна заштита права личности“, *Зборник радова Правног факултета у Нишу*, бр. 68, 2014, стр. 270–271.

личности. Појачана правна заштита ових података не представља произвољно издвајање одређених информација из општег режима заштите, већ последицу процене да њихова обрада може изазвати нарочито интензивне последице по права и слободе појединца²³.

Права личности припадају кругу субјективних права која за предмет имају нематеријална добра непосредно повезана са личношћу њиховог титулара. Њихово теоријско уобличавање представља резултат дугог развоја приватног права, током којег је постепено напуштана традиционална оријентација грађанског права ка претежно имовинским интересима. У класичном грађанском праву заштита правних субјеката била је у значајној мери усмерена на имовинска добра и имовинске интересе. Међутим, развојем правне мисли постепено је прихваћено схватање да човекова правна заштита не може бити ограничена на његову имовинску сферу. Постоје добра која немају непосредну имовинску вредност, али која су за постојање и развој личности од суштинског значаја. Управо таква добра постају предмет права личности.²⁴

Симоновић и Лазић указују на то да су права личности најмлађи члан породице грађанских апсолутних субјективних права и да њихово признавање обезбеђује непосредну правну власт и контролу над личним добрима, међу којима посебно истичу живот, интегритет, достојанство и приватност. Истовремено, указују на њихову повезаност са различитим гранама права, јер се њихова заштита остварује посредством уставног, грађанског, кривичног и управног права²⁵. Наведено схватање од посебног је значаја за право заштите података о личности. Податак који се односи на физичко лице не представља само информацију у техничком или чињеничном смислу. Он може бити средство идентификације, описивања, процене или класификације одређеног лица, а самим тим може имати непосредан утицај на његов правни и фактички положај. Када се одређена информација односи на здравље, генетске или биометријске карактеристике, политичка, верска или филозофска уверења, сексуални живот или сексуалну оријентацију лица, веза између информације и личности постаје још непосреднија.

²³ Андоновић, С., Прља, Д., *Основи права заштите података о личности*, Београд, Институт за упоредно право, 2020, стр. 66–73;

²⁴ Симоновић, И., Лазић, М., „Грађанскоправна заштита права личности“, *Зборник радова Правног факултета у Нишу*, бр. 68, 2014, стр. 270–271.

²⁵ Ibidem стр. 270-272.

Једна од основних вредности на којима почива савремена концепција права личности јесте људско достојанство. Иако се достојанство не може свести на једно конкретно субјективно право, оно представља фундаменталну вредносну основу великог броја права која имају за циљ заштиту човека као слободног и аутономног бића.

У контексту заштите података, достојанство подразумева да човек не може бити сведен на објекат прикупљања, складиштења, анализирања и комерцијалног или административног искоришћавања информација. Појединац остаје носилац права и онда када се његови подаци обрађују у оквиру сложених информационих система.

Заштита достојанства зато захтева да се са подацима који су тесно повезани са идентитетом лица поступа уз нарочиту правну пажњу. У том смислу, појачана заштита посебних категорија података представља један од начина да се правно операционализује начело поштовања личности. Достојанство, међутим, не треба посматрати изоловано од аутономије. Ако достојанство подразумева признавање човека као вредности саме по себи, аутономија подразумева признавање његове способности да самостално доноси одлуке о питањима која се тичу његовог живота. У области података, ова два принципа се спајају кроз идеју **информационог самоодређења**, која је детаљно разрађена у пресуди Савезног уставног суда Немачке од 15. децембра 1983. године.²⁶

Суштина овог концепта није у томе да појединац има апсолутно право да одлучује о свакој информацији која се односи на њега. Такав приступ био би практично неодржив у савременом друштву. Лични подаци се нужно обрађују у здравству, образовању, радним односима, јавним службама, правосуђу, социјалној заштити, финансијском систему и бројним другим областима. Дакле, суштина информационог самоодређења је у томе што оно представља правно уређену могућност појединца да буде упознат са обрадом својих података, да разуме њену сврху, да под одређеним условима утиче на њу и да користи правна средства у случају незаконитог поступања.

²⁶ Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 u. a., *BVerfGE* 65, 1-88.

У правној доктрини поставља се питање да ли право на заштиту података о личности треба схватити као посебан облик права на приватност или као самостално људско право. Ово питање није само теоријско, јер од начина његовог решавања зависи и разумевање предмета правне заштите.

Према једном приступу, заштита података представља посебан аспект права на приватност. Према овом схватању, предмет заштите остаје везан за приватну сферу појединца, док се правила о заштити података посматрају као механизам заштите од неовлашћеног прикупљања, употребе и откривања информација које се односе на приватни живот.

Међутим, постоји снажна основа за схватање да право на заштиту података има самосталну правну природу. То се посебно види у европском праву, где су право на приватност и право на заштиту података нормативно раздвојени. Такво раздвајање није случајно. Оно показује да предмет заштите није идентичан. Право на приватност усмерено је пре свега на заштиту приватне сфере живота, док право на заштиту података регулише услове под којима се информације које се односе на физичко лице могу прикупљати, чувати, користити, мењати, откривати или на други начин обрађивати.

Посебна нормативна потврда овог приступа садржана је у Општој уредби о заштити података Европске уније (GDPR), која успоставља систем начела обраде, права лица на које се подаци односе, обавеза руковалаца и обрађивача и механизма надзора. Такав систем не би био неопходан у истој мери када би се заштита података свела искључиво на класично право на приватност. Стога се може закључити да су приватност и заштита података функционално повезана, али концептуално различита права.

Посебан теоријски аспект савремене заштите података представља питање **информационе асиметрије**²⁷. У традиционалним правним односима претпоставља се да стране у одређеној мери могу да знају садржину и последице својих поступака. Код савремене обраде података та претпоставка често није реална. Појединац неретко не зна које све информације одређени субјект поседује о њему, на који начин су оне прикупљене,

²⁷ Paul van der Waerd, „Information asymmetries: recognizing the limits of the GDPR on the data-driven market“, *Computer Law & Security Review*, vol. 38, 2020, art. 105436.

са којим другим информацијама су повезане и за које се све сврхе користе. Насупрот томе, велики информациони системи могу располагати огромним количинама података и средствима за њихову анализу. Таква асиметрија ствара неравнотежу моћи. Због тога савремено право заштите података настоји да успостави институционалну противтежу. Обавезе транспарентности, права приступа, исправке, брисања података, ограничења обраде и друга права лица на које се подаци односе имају, између осталог, функцију смањења информационе асиметрије. У том смислу, заштита података није само право на приватност, већ и механизам ограничења информационе моћи.

Један од темељних принципа савременог права заштите података јесте **ограничење сврхе**. Подаци се не прикупљају и не обрађују у апстрактном смислу, већ за конкретно одређену и легитимну сврху. Ако је лице дало одређену информацију у једном контексту и за одређену сврху, онда се њена даља употреба мора посматрати у односу на ту сврху. Промена сврхе може представљати суштинску промену односа у којем је информација првобитно дата. Начело ограничења сврхе посебно добија на значају код посебних података. Када се податак односи на здравље, генетске или биометријске карактеристике, уверења или сексуални живот лица, промена контекста и сврхе обраде може значајно повећати ризик по његова права.

Са ограничењем сврхе тесно је повезано начело **минимизације података**. Оно подразумева да се не треба прикупљати податке у ширем обиму него што је неопходно за остварење легитимне сврхе. Што је већа количина података која се прикупља, већи је и број потенцијалних последица њихове злоупотребе. Ово је посебно изражено када се подаци међусобно повезују и када се из њих изводе нове информације.

Посебна правна заштита одређених категорија података може се теоријски објаснити применом принципа **приступа заснованог на ризику** (енг. risk-based approach). Не носе сви подаци исти потенцијал за угрожавање основних права и слобода. Подаци који се односе на здравље, генетске податке, биометријске податке који се обрађују ради јединствене идентификације, политичка и верска уверења, синдикално чланство, сексуални живот или сексуалну оријентацију лица могу, зависно од околности, бити извор нарочито озбиљних последица.

Један од кључних разлога за појачану заштиту посебних категорија података лежи у опасности од дискриминације. Одређени лични подаци могу открити својства која су у непосредној вези са једнакошћу и равноправношћу лица. У том смислу, право заштите података о личности има шири друштвени значај. Оно не штити само право појединца да одређену информацију задржи за себе, већ и његово право да не буде неповољно третиран због информације која се односи на његову личност.

Развој дигиталних технологија додатно је усложио проблематику заштите података. Савремени системи могу обрађивати огромне количине информација и из њих изводити закључке који нису непосредно садржани у појединачним подацима. На тај начин, информациона вредност једног податка више није ограничена на његову непосредну садржину. Његовом комбинацијом са другим подацима могу се добити нове информације о појединцу.

Проблем је нарочито значајан у контексту великих података. Европски надзорник за заштиту података посветио је посебну пажњу односу Big Data технологија и заштите података, указујући на озбиљне ризике које обрада великих количина података може имати за права и слободе појединаца и на потребу доследне примене принципа заштите података у окружењу Big Data.²⁸ У том контексту нарочито су значајни принципи ограничења сврхе, минимизације података, транспарентности и одговорности.

Једна од најзначајнијих последица наведених теоријских схватања јесте прелаз са реактивног на превентивни модел заштите.

Класична грађанскоправна заштита права личности у великој мери је усмерена на отклањање последица повреде. Међутим, код обраде података такав приступ није увек довољан. Када је једном дошло до откривања осетљивог податка, новчана накнада штете не може увек у потпуности вратити ситуацију у претходно стање. Симоновић и Лазић управо указују на значај разликовања превентивне и реактивне заштите права личности.

²⁸ European Data Protection Supervisor (EDPS), *Opinion 7/2015: Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability*, 19 November 2015, стр. 7–8.

Према њиховом приступу, правна заштита мора омогућити како спречавање повреде тако и отклањање њених последица²⁹.

Право на заштиту података о личности, као и друга основна права, није апсолутно у свим својим аспектима. Савремено друштво захтева обраду података у бројним областима. Због тога правни поредак мора успоставити равнотежу између заштите личности и других легитимних интереса. **Принцип пропорционалности** представља један од основних инструмената за успостављање те равнотеже. Обрада мора бити усмерена на легитиман циљ, погодна за његово остварење, неопходна и сразмерна. Код посебних података овај захтев добија нарочиту тежину. Што је већи потенцијални ризик по права појединца, то мора бити убедљивије оправдање за обраду и снажније гаранције заштите.

Савремена доктрина заштите података о личности може се, у крајњем, посматрати као резултат постепеног проширивања концепта правне заштите личности. Почетно тежиште било је на физичком и моралном интегритету, затим на приватности, да би се у информационом друштву све већи значај придао информационој димензији личности. Тај развој није довео до потискивања традиционалног права на приватност. Напротив, приватност је остала један од основних темеља савремене заштите података. Међутим, она више није довољна да обухвати све облике ризика које савремена технологија ствара.

1.3 Права личности у уставноправном систему Републике Србије

Права личности представљају једну од најзначајнијих категорија субјективних права у савременом правном поретку. Њихов значај произлази из чињенице да су усмерена на заштиту човека као физичког, психичког, моралног и друштвеног бића, односно на заштиту његовог живота, телесног и психичког интегритета, части, угледа, достојанства, приватности, идентитета и других добара која су нераскидиво повезана са личношћу. За разлику од имовинских права, чији је непосредни предмет одређена имовинска вредност, права личности штите нематеријална добра која чине суштински део човекове индивидуалности и његовог положаја у друштву.

²⁹ Симоновић, И., Лазић, М., „Грађанскоправна заштита права личности“, *Зборник радова Правног факултета у Нишу*, бр. 68, 2014, стр. 281.

У савременим правним системима права личности имају вишеструку правну природу. Она се истовремено појављују као уставом зајемчена људска права, као грађанска субјективна права, као основ за примену кривичноправних и управноправних механизма заштите, али и као полазиште за регулисање посебних области друштвених односа, као што су радни односи, здравствена заштита, породични односи, електронске комуникације и делатност органа јавне власти. Та сложена правна природа условљена је чињеницом да се повредом једног личног добра истовремено може нарушити више различитих правних интереса појединца.

Устав Републике Србије из 2006. године права личности не уређује у једној јединственој и затвореној целини, већ их гарантује кроз више међусобно повезаних уставних одредаба. Устав полази од начела владавине права, непосредне примене људских и мањинских права и забране дискриминације, а затим посебно гарантује људско достојанство и слободан развој личности, право на живот, неповредивост физичког и психичког интегритета, неповредивост стана, тајност писама и других средстава комуницирања, заштиту података о личности, као и слободу мисли, савести и вероисповести³⁰. Наведене гаранције чине међусобно повезан нормативни оквир за заштиту различитих аспеката личности. У том смислу, права личности у уставноправном систему Републике Србије треба посматрати као целовит систем правних гаранција чији је основни циљ очување аутономије појединца и заштита његовог достојанства.

Развој информационих технологија, дигитализација јавне управе, електронско пословање, масовна обрада података и све већа употреба аутоматизованих система довели су до тога да подаци о личности постану један од најзначајнијих објеката правне заштите. Појединац више није изложен само традиционалним облицима повреде приватности, као што су неовлашћено објављивање писама, фотографија или података из приватног живота, већ и сложеним облицима обраде података, профилисања, повезивања база података, праћења понашања и доношења одлука на основу аутоматизоване анализе. Због тога уставноправна заштита личности данас обухвата не само заштиту од непосредног

³⁰ Устав Републике Србије, „Службени гласник РС“, бр. 98/2006, чл. 3, 18, 21, 23–25, 40–43.

уплитања у приватни живот, већ и заштиту од неконтролисаног прикупљања, чувања, коришћења и размене информација о појединцу.

Начело непосредне примене људских и мањинских права, садржано у члану 18. Устава, додатно потврђује да се уставом зајемчена права не могу схватити само као програмске норме или политичке декларације. Тумачећи ову одредбу, можемо рећи да је сам њен циљ истицање чињенице да права требају бити применљива и обавезују сваки орган јавне власти, али и друге субјекте. Овакав уставни постулат има посебну важност у области заштите података о личности. Устав изричито предвиђа да се прикупљање, држање, обрада и коришћење података о личности уређују законом. Законодавац је дужан да успостави нормативни оквир који омогућава остваривање права, а не да га сведе на формалну гаранцију. То подразумева јасно одређивање услова под којима је обрада података дозвољена, утврђивање права лица на које се подаци односе, прописивање обавеза руковалаца и обрађивача, као и обезбеђивање независног надзора и делотворних правних средстава.

Права личности су у Уставу заштићена и кроз опште одредбе о људском достојанству, забрани дискриминације и слободном развоју личности. Члан 23. Устава утврђује да је људско достојанство неприкосновено и да су сви дужни да га поштују и штите. Достојанство представља општи вредносни темељ свих права личности. Оно подразумева да се човек не сме свести на објект туђе воље, на средство за остваривање туђих циљева или на обичан скуп података који се могу неограничено прикупљати и користити без обзира на последице по његов положај.

Уставна забрана дискриминације, садржана у члану 21, такође је од непосредног значаја за заштиту права личности. Обрада података може довести до дискриминаторног поступања у области запошљавања, образовања, здравствене заштите, социјалне сигурности, осигурања, банкарских услуга или приступа јавним услугама. Посебан ризик постоји када се обрађују подаци који откривају расно или етничко порекло, верска или филозофска уверења, политичка мишљења, чланство у синдикату, здравствено стање, генетске и биометријске карактеристике, сексуални живот или сексуалну оријентацију.

Због тога заштита података о личности није само питање приватности, већ и средство спречавања неједнаког и неправичног поступања.

Уставна заштита права личности има и вертикалну и хоризонталну димензију. Вертикална димензија односи се на однос појединца и државе, односно на обавезу државних органа да се уздрже од неовлашћеног мешања у личну сферу појединца и да предузму мере ради њене заштите. Хоризонтална димензија односи се на односе између приватних лица. Она је посебно значајна у случајевима када послодавац, здравствена установа, банка, интернет-платформа, привредно друштво или друго правно лице обрађује податке о физичком лицу. У том контексту, уставне гаранције права личности не исцрпљују се у односу према држави. Држава има позитивну обавезу да успостави правни систем који ће омогућити заштиту појединца и у односима са другим приватним субјектима. То се остварује кроз законско уређивање грађанскоправне одговорности, заштите потрошача, радних односа, здравствене документације, електронских комуникација, безбедности информационих система и других области у којима се обрађују подаци о личности.

Право на приватност представља једно од основних права личности. Његов садржај обухвата заштиту приватног и породичног живота, дома, преписке, комуникација, личних односа, интимне сфере, телесног и психичког интегритета, као и могућности појединца да самостално одлучује о томе које информације о њему могу бити доступне другим лицима.

Право на заштиту података о личности тесно је повезано са правом на приватност, али се са њим не може у потпуности изједначити. Приватност представља ширу правну и друштвену категорију, док је право на заштиту података о личности усмерено на контролу и законитост поступања са информацијама које се односе на одређено или одредиво физичко лице³¹. За повреду права на заштиту података није неопходно да дође до откривања интимне или строго приватне чињенице. Довољно је да се подаци прикупљају,

³¹ Gloria González Fuster, Paul De Hert, „The Legal Construction of Privacy and Data Protection“, *Computer Law & Security Review*, vol. 29, no. 5, 2013, стр. 522–530.

чувају, користе или откривају супротно закону, без одговарајућег правног основа, изван утврђене сврхе или на начин који угрожава права и слободе лица³².

У том смислу, податак о личности може бити и информација која сама по себи није интимна, односно није осетљивог карактера. Име, адреса, број телефона, број личног документа, подаци о запослењу, подаци о кретању или идентификатор електронског уређаја могу постати значајни са становишта заштите личности ако се повежу са другим подацима, употребе за профилисање или примене у одлучивању о правима и обавезама појединца. Савремени приступ заштити података зато не полази само од садржине податка, већ и од начина његове обраде, контекста, сврхе и могућих последица.

Члан 42. Устава представља централну уставноправну норму у области заштите података о личности. Његова прва реченица гласи: „Зајемчена је заштита података о личности.“ Оваква формулација потврђује да заштита података није само део општег права на приватност, већ посебно уставно право. Други став члана 42. прописује да се прикупљање, држање, обрада и коришћење података о личности уређују законом. Овом одредбом успостављен је принцип законске резерве. То значи да се питања која се односе на обраду података не могу препустити искључиво интерним правилима органа, одлукама привредних субјеката или неформалној пракси. Неопходно је постојање закона који јасно одређује услове обраде, права лица и обавезе субјеката који податке обрађују. Трећи став члана 42. садржи једно од најважнијих начела заштите података, и то забрану и кажњивост употребе података изван сврхе за коју су прикупљени. Ово правило изражава начело ограничења сврхе, према којем се подаци могу прикупљати за одређене, изричите и законите сврхе и не могу се накнадно користити на начин који је неспојив са првобитном сврхом. Одступања су могућа за потребе вођења кривичног поступка или заштите безбедности Републике Србије, али само на начин предвиђен законом.

Овакво уставно решење има двоструки значај. С једне стране, оно штити појединца од произвољног ширења сврхе обраде. С друге стране, оно омогућава да се у посебно оправданим ситуацијама подаци користе ради заштите важних јавних интереса. Међутим,

³² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Art. 5(1), 6(1) и 9(1).

позивање на јавни интерес не може бити неограничено. Свако одступање мора бити засновано на јасној правној норми, оправдано легитимним циљем и подвргнуто захтевима неопходности, сразмерности и контроле.

Четврти став члана 42. гарантује право сваког лица да буде обавештено о подацима који су прикупљени о његовој личности, као и право на судску заштиту због њихове злоупотребе. Право на обавештеност представља предуслов остваривања других права. Појединац не може захтевати исправку нетачних података, брисање незаконито обрађених података или ограничење обраде ако не зна ко његове податке обрађује, у које сврхе, на основу ког правног основа и у ком обиму. Право на судску заштиту потврђује да уставна гаранција није потпуна без делотворног правног средства. Заштита мора бити доступна у случају незаконите обраде, неовлашћеног откривања, злоупотребе података, ускраћивања приступа подацима, неоправданог одбијања исправке или брисања, као и у случајевима када обрада података доведе до повреде других права и слобода. Судска заштита се при томе допуњује механизмима управног надзора, поступањем Повереника за информације од јавног значаја и заштиту података о личности, као и грађанскоправним, прекршајним и кривичноправним средствима.

Посебни подаци о личности, односно посебне врсте података о личности, представљају категорију података чија обрада може нарочито озбиљно угрозити достојанство, приватност, равноправност и друга права појединца. Њихова посебност не произлази само из саме природе информација, већ и из могућности да њихова злоупотреба доведе до дискриминације, стигматизације, социјалне искључености, нарушавања професионалног и породичног живота или угрожавања телесног и психичког интегритета. Њихова обрада по правилу подлеже строжим условима и додатним гаранцијама.

Посебни подаци о личности имају непосредну везу са више уставних права. Подаци о здравственом стању повезани су са правом на неповредивост физичког и психичког интегритета, правом на приватност и правом на здравствену заштиту. Подаци о политичким мишљењима повезани су са слободом мисли, савести, уверења и изражавања. Подаци о верским уверењима повезани су са слободом вероисповести и правом лица да се не изјашњава о својим уверењима. Подаци о сексуалном животу и сексуалној оријентацији

повезани су са правом на приватни и породични живот, достојанством и забраном дискриминације.

Посебан режим заштите ових података оправдан је чињеницом да њихова злоупотреба може имати последице које превазилазе обичан губитак контроле над информацијом. Објављивање података о здравственом стању може довести до нарушавања угледа или дискриминације на раду; откривање политичких или верских уверења може угрозити слободу савести; неовлашћено откривање података о сексуалном животу може изазвати тешке последице по приватност, породичне односе и психички интегритет лица.

Устав Републике Србије не издваја посебне податке о личности у посебну категорију у оквиру члана 42, али се њихова појачана заштита изводи из опште уставне гаранције заштите података, начела људског достојанства, забране дискриминације, права на приватност, слободе мисли и вероисповести, као и других релевантних права. Закон о заштити података о личности зато предвиђа посебне услове за њихову обраду, имајући у виду повећан ризик који они носе.

На крају, може се закључити да уставноправна заштита права личности у Републици Србији почива на споју општих уставних начела, посебних права и законских механизма заштите. Њена делотворност зависи не само од постојања нормативних гаранција, већ и од њихове доследне примене у пракси, независног надзора, доступности судске заштите и развијања културе одговорног поступања са подацима. У том контексту, заштита посебних података о личности представља један од најосетљивијих сегмената савременог система права личности, јер се кроз њу непосредно штите достојанство, аутономија, равноправност и слободан развој сваког појединца.

II ПОЈАМ И ЗНАЧАЈ ПОСЕБНИХ ПОДАТАКА О ЛИЧНОСТИ

Посебне врсте података о личности представљају посебно осетљив сегмент савременог система заштите података, будући да њихова садржина непосредно задире у најдубље и најинтимније сфере човекове личности. За разлику од података који се односе на појединца у ширем смислу, посебне врсте података откривају или могу открити његово

здравствено стање, генетске и биометријске карактеристике, расно или етничко порекло, политичка мишљења, верска или филозофска уверења, синдикалну припадност, сексуални живот или сексуалну оријентацију. Управо зато њихова правна природа није одређена само информационим садржајем, већ и степеном ризика који њихова обрада може произвести по достојанство, приватност, аутономију и равноправност појединца.

У правном поретку Републике Србије посебне врсте података о личности уређене су чланом 17. Закона о заштити података о личности, који полази од начелне забране њихове обраде, али истовремено предвиђа законом утврђене изузетке³³. На тај начин законодавац успоставља строжи правни режим који се заснива на идеји да повећана осетљивост података захтева и повећани степен правне заштите. Слично решење садржано је и у члану 9. Опште уредбе о заштити података, која обраду посебних категорија личних података начелно забрањује, допуштајући је само под посебно прописаним условима³⁴.

Значај посебних података, међутим, не произлази само из чињенице да се они односе на осетљиве аспекте личности. Њихова посебна правна тежина лежи у могућности да се њиховом злоупотребом појединцу припишу одређена својства, да се донесу одлуке које утичу на његов правни или друштвени положај, или да се створи основ за различито поступање и дискриминацију.

У том смислу, посебни подаци представљају својеврсну **информациону интиму личности**. Као што право штити човеково тело од недозвољеног физичког захвата, тако и право заштите података настоји да постави границе недозвољеном продору у информациони слој његове личности. Што је информација дубље повезана са идентитетом, здрављем, уверењима или интимним животом појединца, то је оправданији захтев да њена обрада буде подвргнута строжим правним условима и снажнијим гаранцијама. У томе се и огледа суштина посебног режима заштите - не штити се само податак као информација,

³³ Закон о заштити података о личности, „Службени гласник РС“, бр. 87/2018, чл. 17, ст. 1–2;

³⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (*General Data Protection Regulation*), Art. 9(1)–(2).

већ човекова могућност да остане слободан од нежељеног откривања, категоризације и употребе најосетљивијих сазнања о себи.³⁵

Посебна осетљивост ових података добија додатну тежину у савременом дигиталном окружењу. Савремене технологије омогућавају да се подаци који су некада постојали одвојено повежу, анализирају и употребе за извођење нових закључака о појединцу. Због тога ризик више не произлази искључиво из непосредног откривања одређене информације, већ и из могућности да се њеним комбиновањем са другим подацима изгради детаљан профил личности.

Из перспективе правне теорије, значај посебних података зато превазилази оквир једног института права заштите података. Они представљају место сусрета технолошког развоја и најстаријих правних захтева заштите личности. У њима се најдиректније поставља питање колико право може дозволити да информације о човеку буду предмет сазнања, обраде и употребе, а да се при том не наруши његова аутономија. У том смислу, степен заштите који један правни поредак пружа посебним врстама података може се посматрати и као показатељ његове способности да у условима све веће информатизације очува суштину права личности.³⁶

Најзад, посебне врсте података показују да се граница између приватности и технологије све више помера са питања „ко шта зна о човеку“ ка сложенијем питању „шта све из онога што се о човеку зна може бити закључено, предвиђено и учињено“. Управо у том померању лежи њихов савремени правни значај. Право зато не штити само тајну о човеку, већ и његову слободу да не буде сведен на скуп информација из којих други могу изводити закључке о његовом идентитету, вредностима, здрављу или животу.

2.1 Дефиниција и класификација посебних података о личности

Појам посебних података о личности представља једно од централних питања савременог права заштите података о личности. Његово правилно одређивање захтева претходно разумевање ширег појма податка о личности, будући да посебне врсте података

³⁵ Paul Quinn, Gianclaudio Malgieri, „The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework“, *German Law Journal*, vol. 22, no. 8, 2021, стр. 1583–1585.

³⁶ Ibidem, стр. 1592-1594.

представљају његову ужу, квалификовану категорију. Другим речима, сваки податак који припада посебној категорији истовремено је и податак о личности, али сваки податак о личности нема својство посебне врсте података.

Закон о заштити података о личности Републике Србије (у даљем тексту: ЗЗПЛ) прихвата широко одређење податка о личности. 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 су 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 идентитета³⁷. Из наведене дефиниције произлази да је за постојање податка о личности одлучујућа његова повезивост са одређеним или одредивим физичким лицем, а не форма у којој је информација садржана. Податак може постојати у писаном, електронском, аудио-визуелном, биометријском или другом облику. Такође, није неопходно да сам податак непосредно открива идентитет лица. Довољно је да се идентитет може утврдити непосредно или посредно, коришћењем одређених додатних информација.

Ово широко одређење има нарочит значај у савременом информационом друштву. Развој дигиталних технологија довео је до тога да велики број информација које на први поглед не садрже име или презиме лица ипак може бити повезан са одређеним појединцем. Идентификатори у електронским комуникацијама, подаци о локацији, интернет идентификатори, подаци о уређају који лице користи, подаци о његовим навикама и различити технички трагови могу, када се посматрају појединачно или у комбинацији, омогућити идентификацију физичког лица.

Посебне врсте података о личности представљају подкатегорију података о личности која ужива појачану правну заштиту због природе података и повећаног ризика који њихова обрада може представљати за права и слободе физичког лица. У домаћој литератури и пракси могу се сусрести различити називи за ову категорију. Поред законског израза „посебне врсте података о личности“, користе се и термини „осетљиви

³⁷ Закон о заштити података о личности, „Службени гласник РС“, бр. 87/2018, чл. 4. ст. 1. тач. 1.

подаци“, „осетљиви лични подаци“ и „посебне категорије података“. Иако термилошке разлике постоје, њима се у највећем броју случајева означавају подаци чија обрада због своје природе може довести до нарочито озбиљног угрожавања основних права и слобода појединца.

Разлог за издвајање ових података лежи у чињеници да они откривају одређене особине, уверења или карактеристике које су тесно повезане са идентитетом, аутономијом, приватношћу и достојанством човека. Њихова незаконита обрада може довести до дискриминације, стигматизације, нарушавања угледа, социјалне искључености, ограничења приступа одређеним услугама или правима, као и других последица које могу бити знатно озбиљније од последица обраде података који немају такав карактер.

Посебност ових података, међутим, не треба схватити тако да су они у апсолутном смислу „опасни“ или да је свака њихова обрада забрањена. Њихова посебност пре свега се огледа у томе што законодавац захтева виши степен оправданости и додатне услове за њихову обраду. ЗЗПЈ у члану 17. полази од правила забране обраде посебних врста података, након чега у наредним одредбама предвиђа ситуације у којима је таква обрада, под одређеним условима, дозвољена.

Исти нормативни приступ прихвата и право Европске уније. Члан 9. Опште уредбе о заштити података (GDPR) утврђује забрану обраде посебних категорија података, али истовремено предвиђа таксативно одређене изузетке. На тај начин систем заштите није заснован на апсолутној забрани, већ на појачаном режиму заштите. Директива 95/46/ЕЗ, која је претходила GDPR-у³⁸, такође је посебне категорије података издвојила у посебан режим, што показује континуитет развоја европског права заштите података.

Концепт посебних категорија података није настао тек доношењем GDPR-а. Његови корени налазе се у ранијим европским и међународним инструментима заштите приватности и података о личности. Посебан значај има Конвенција Савета Европе о заштити лица у односу на аутоматску обраду података о личности из 1981. године, позната

³⁸ Директива 95/46/ЕЗ Европског парламента и Савета од 24. октобра 1995. године о заштити физичких лица у односу на обраду података о личности и о слободном кретању таквих података, ОЈ L 281, 23. 11. 1995, стр. 31, чл. 8. ст. 1–2;

као Конвенција 108³⁹. Њено доношење представљало је значајан корак у развоју међународних стандарда заштите података о личности. Каснији развој европског права довео је до Директиве 95/46/EЗ, која је посебне категорије података уредила у оквиру члана 8. Директива је предвиђала посебан режим за податке који откривају расно или етничко порекло, политичка мишљења, верска или филозофска уверења, синдикално чланство, као и податке о здрављу и сексуалном животу.

Доношењем GDPR-а⁴⁰ концепт је додатно развијен. У члану 9. проширен је обухват категорија тако да, поред већ наведених, изричито обухвата генетске податке и биометријске податке који се обрађују у циљу јединствене идентификације физичког лица, као и сексуалну оријентацију. На тај начин нормативни систем је прилагођен технолошком развоју и новим ризицима који произлазе из савремених начина обраде података.

ЗЗПЛ је у овом делу у значајној мери преузео концептуални приступ GDPR-а. Члан 17. ЗЗПЛ садржи исту основну листу категорија, што омогућава висок степен упоредивости домаћег и европског правног оквира. То је од посебног значаја имајући у виду европске интеграције Републике Србије и потребу усклађивања националног законодавства са европским стандардима у области заштите података.

Члан 17. ЗЗПЛ представља централну одредбу за одређивање посебних врста података о личности у правном систему Републике Србије. Према овој одредби, посебне врсте података обухватају:

1. податке који откривају расно или етничко порекло;
2. податке који откривају политичко мишљење;
3. податке који откривају верско или филозофско уверење;
4. податке који откривају чланство у синдикату;
5. генетске податке;

³⁹ Конвенција о заштити лица у односу на аутоматску обраду података о личности, ETS бр. 108, Стразбур, 28. јануар 1981. године;

⁴⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4.5.2016, стр. 1–88, Art. 9(1)–(2).

6. биометријске податке у циљу јединствене идентификације физичког лица;
7. податке о здравственом стању;
8. податке о сексуалном животу;
9. податке о сексуалној оријентацији.

Ова класификација може се посматрати према природи информације која се њоме открива. Једну групу чине подаци који се односе на уверења, ставове, припадност или идентитет лица – расно или етничко порекло, политичка мишљења, верска и филозофска уверења и синдикално чланство. Другу групу чине подаци који се односе на биолошке, телесне и интимне карактеристике – генетски, биометријски и здравствени подаци, као и подаци о сексуалном животу и сексуалној оријентацији.

Прву категорију представљају подаци који откривају расно или етничко порекло физичког лица. Њихова посебна заштита заснива се пре свега на опасности од дискриминације и различитог поступања према лицима на основу њиховог порекла. Ова категорија има непосредну везу са уставним начелом забране дискриминације. Информација о етничком или расном пореклу може у одређеним друштвеним и политичким околностима бити злоупотребљена за стигматизацију, издвајање или неједнако поступање према одређеној групи.

Друга категорија односи се на политичка мишљења. Посебна заштита ове категорије има снажну уставноправну основу, јер је повезана са слободом мисли, савести и уверења, слободом изражавања, политичким плурализмом и демократским учешћем грађана. Политичко мишљење може бити изражено непосредно (изјавом, чланком, говором или гласањем у околностима у којима је идентитет гласача познат), али може бити откривено и посредно (на основу активности лица, чланства у политичкој организацији, подршке одређеној иницијативи или других информација). Управо могућност комбиновања различитих података ствара значајан ризик од политичког профилисања. Посебно је значајно да се политичка мишљења не могу свести само на формално чланство у политичкој странци, већ се појам односи на ширу сферу политичких ставова и уверења.

Трећу категорију чине подаци који откривају верско или филозофско уверење. Ови подаци су непосредно повезани са слободом мисли, савести и вероисповести и са правом појединца да самостално одређује своја духовна и вредносна уверења.

Четврта категорија односи се на податке о чланству у синдикату. Њихова заштита повезана је са слободом удруживања и правима из области рада. Чињеница да је лице члан одређеног синдиката може открити његове ставове о условима рада, однос према послодавцу, учешће у колективном преговарању или другим облицима синдикалног деловања. Посебан ризик постоји у радном односу, јер послодавац може доћи у посед информације која, ако се користи на недозвољен начин, може довести до неповољнијег поступања према запосленом.

Пету категорију чине генетски подаци, који представљају једну од најзначајнијих категорија посебних врста података у савременом праву. Њихов значај произлази из специфичне природе генетске информације, која може откривати одређене биолошке карактеристике, предиспозиције и друге информације о физичком лицу. Посебност генетских података огледа се и у чињеници да њихов информациони потенцијал није нужно ограничен само на једно лице. Генетске карактеристике су повезане са наследним особинама, па одређени генетски подаци могу имати значај и за биолошке сроднике лица. Развој генетичких тестова, персонализоване медицине и комерцијалних генетичких анализа додатно повећава значај правне заштите ове категорије.

Шеста категорија односи се на биометријске податке, који представљају посебну категорију због тога што се односе на физичке, физиолошке или понашајне карактеристике лица које омогућавају или олакшавају његову идентификацију. Међутим, веома је важно нагласити да није сваки биометријски податак аутоматски посебна врста података. Према ЗЗПЛ-у, посебну категорију представљају биометријски подаци који се обрађују у циљу јединствене идентификације физичког лица. Ова разлика је од великог практичног значаја. На пример, сама фотографија лица не мора по аутоматизму представљати посебну врсту података. Она то може постати када се обрађује специфичним техничким средствима на начин који омогућава или служи јединственој идентификацији лица. Биометријски подаци носе специфичан ризик јер су непосредно повезани са самим телом лица. За разлику од

лозинке или идентификационог броја, биометријску карактеристику није могуће једноставно „променити“ у случају компромитовања. Због тога злоупотреба биометријских података може имати дуготрајне последице.

Подаци о здравственом стању, **седма категорија**, спадају међу најосетљивије категорије посебних података, јер су непосредно повезани са приватношћу, физичким и психичким интегритетом и достојанством лица. Обухватају информације о здравственом стању, болестима, дијагнозама, терапијама и медицинским поступцима, а њихова неовлашћена обрада може довести до дискриминације и других неповољних последица, нарочито у радном односу, осигурању и другим областима живота. Дигитализација здравствене документације додатно повећава значај ограничења приступа, јер омогућава брзо повезивање, копирање и преношење великог броја здравствених података.⁴¹ Неовлашћено откривање здравствених података може имати последице у радном односу, приликом закључивања уговора о осигурању, у породичним односима и другим областима живота. Због тога је неопходно да приступ здравственим подацима буде ограничен на лица која за то имају одговарајући правни основ и стварну потребу. Питање заштите здравствених података посебно је значајно у контексту електронских здравствених система. Дигитализација здравствене документације доноси бројне предности, али истовремено ствара ризик од неовлашћеног приступа, копирања, преноса и повезивања података⁴². Због тога се правна заштита мора допуњавати одговарајућим техничким и организационим мерама.

Осму категорију чине подаци који се односе на сексуални живот и сексуалну оријентацију физичког лица. Реч је о подацима који су непосредно повезани са интимном сфером личности и чије неовлашћено откривање може имати изузетно озбиљне последице по приватност, достојанство и друштвени положај лица. Заштита ових података заснива се на идеји да појединац има право да самостално одређује коме ће открити информације о свом интимном животу. Посебан ризик постоји у случају објављивања таквих информација без пристанка лица, али и у случају њиховог коришћења ради профилисања

⁴¹ К. Дулчић, Н. Бодигог-Вукобрат, „Заштита особних података пацијената у еуропском и хрватском праву“, стр. 371–411.

⁴² М. Беванда, М. Чолаковић, „Правни оквир за заштиту особних података у праву Европске Уније“, Зборник Правног факултета Универзитета у Ријеци, стр. 128-129;

или доношења одлука које могу довести до дискриминације. Значај ове категорије додатно се повећава у дигиталном окружењу, у којем једном објављена или компромитована информација може бити умножена и даље дистрибуирана великом броју лица.

Приликом класификације посебних врста података неопходно је направити разлику између података из члана 17. ЗЗПЛ и података о кривичним пресудама и кажњивим делима из члана 19. ЗЗПЛ⁴³. Подаци о кривичним пресудама и кажњивим делима нису наведени у члану 17. међу посебним врстама података, али им закон такође обезбеђује посебан режим заштите. Овакво нормативно решење је логично јер информације о осуђиваности, кривичним делима или другим кажњивим радњама могу имати озбиљне последице по друштвени и професионални положај лица. Разлика је, дакле, у правној класификацији. Посебне врсте података из члана 17. односе се на одређена лична својства, уверења и биолошке или интимне карактеристике, док се подаци из члана 19. односе на кривичноправни статус лица и његову повезаност са кривичним делима или кажњивим радњама.

Основна разлика између обичних података о личности и посебних врста података огледа се у степену ризика за права и слободе физичког лица. Обичан податак о личности такође ужива законску заштиту и његова обрада мора испуњавати услове законитости. Међутим, за посебне врсте података постоји додатни ниво заштите. Њихова обрада није довољно оправдана само постојањем општег правног основа за обраду, већ мора постојати и посебан услов предвиђен законом⁴⁴.

Посебна правна заштита посебних врста података може се објаснити кроз неколико међусобно повезаних разлога. Први разлог представља *могућност дискриминације*. Одређене информације, нарочито о пореклу, политичким и верским уверењима, здрављу или сексуалној оријентацији, могу бити употребљене за различито поступање према појединцу. Други разлог представља *заштита људског достојанства*. Подаци о здрављу, сексуалном животу, генетским карактеристикама или верским уверењима непосредно се односе на најинтимније аспекте личности и због тога захтевају посебну правну пажњу.

⁴³ Закон о заштити података о личности, „Службени гласник РС“, бр. 87/2018, чл. 19.

⁴⁴ Ibidem, чл. 12. ст. 1. и чл. 17. ст. 1–2.

Трећи разлог представља *аутономија појединца*. Лице мора имати могућност да у разумној мери одлучује које информације о њему могу бити доступне другима и у које сврхе могу бити коришћене. Четврти разлог односи се на *могућност дуготрајних или неповратних последица*. Ово је нарочито изражено код генетских и биометријских података. Једном компромитовани подаци овог типа не могу се једноставно заменити на начин на који се може променити лозинка или други тајни идентификатор. И коначно, пети разлог представља *могућност секундарне употребе података*. Подаци прикупљени у једну сврху могу бити употребљени за другу сврху, нарочито ако се повежу са другим базама података. Управо због тога принцип ограничења сврхе има посебан значај код посебних врста података.

Свака од наведених категорија посебних података о личности има своју специфичну правну и друштвену димензију. Подаци о расном или етничком пореклу, политичким и верским уверењима и синдикалном чланству нарочито су повезани са слободом, равноправношћу и забраном дискриминације. Генетски и биометријски подаци носе специфичне ризике због своје трајне и јединствене повезаности са телом и идентитетом лица. Подаци о здравственом стању повезани су са телесним и психичким интегритетом, док су подаци о сексуалном животу и сексуалној оријентацији непосредно везани за интимну сферу личности.

2.2 Посебни подаци и њихова улога у заштити приватности

Право на приватност представља једно од основних права личности и једну од темељних вредности савременог правног поретка. Његов значај нарочито долази до изражаја у условима савременог информационог друштва, у којем се о физичким лицима прикупљају, складиште, анализирају и размењују велике количине података. У таквом окружењу граница између приватне и јавне сфере постаје све сложенија, док могућност појединца да самостално контролише информације које се односе на њега добија све већи значај. Посебне врсте података о личности у том контексту заузимају нарочито место, будући да њихова обрада може непосредно задрети у најосетљивије области човековог приватног живота.

Приватност се традиционално схвата као право појединца да буде заштићен од неовлашћеног мешања у његов лични и породични живот, дом и комуникацију. Међутим, савремено схватање приватности превазилази класичну представу о приватности као „праву да се буде остављен на миру“⁴⁵. Развој информационих технологија довео је до тога да се приватност све више посматра и као право појединца да контролише информације које се односе на његову личност, да зна ко те информације прикупља, у коју сврху их користи и коме их ставља на располагање.

Посебни подаци имају посебан значај у овом контексту јер не откривају само основне идентификационе чињенице о појединцу, већ могу открити његова уверења, здравствено стање, биолошке карактеристике, политичке ставове, припадност синдикату, сексуални живот или сексуалну оријентацију. На тај начин они непосредно задиру у сфере личности које појединац по правилу има посебан интерес да контролише. Управо због тога се заштита ових података не може посматрати искључиво као питање техничке безбедности информација, већ као питање заштите основних права и слобода човека.

Код посебних врста података, повреда приватности може постојати и без незаконите обраде података, као што је случај са одређеним облицима неовлашћеног уласка у приватни простор или откривања чињеница из интимног живота. С друге стране, може постојати повреда права на заштиту података и када се не открива информација која је у традиционалном смислу интимна. Због тога право на заштиту података о личности представља шири регулаторни механизам од саме заштите приватности. Оно не реагује само када је приватна информација већ откривена, већ настоји да унапред уреди читав процес поступања са подацима. Уместо да се заштита активира тек након настанка повреде, систем заштите података уводи превентивна правила која се примењују од тренутка прикупљања података.

Та превентивна функција посебно је значајна код посебних врста података. Уколико би се чекало да здравствени подаци, генетске информације, подаци о политичким или верским уверењима или информације о сексуалном животу буду злоупотребљени, накнадна правна заштита често не би могла у потпуности да отклони последице. Једном

⁴⁵ Samuel D. Warren, Louis D. Brandeis, „The Right to Privacy“, *Harvard Law Review*, vol. 4, br. 5, 1890, стр. 195.

објављена информација може бити даље умножена, сачувана, прослеђена и коришћена у другим контекстима. Због тога је код ових података нарочито значајан принцип превенције.

Једна од основних функција заштите посебних података јесте очување аутономије појединца. Аутономија подразумева способност лица да самостално доноси одлуке о сопственом животу, уверењима и личним односима, без неоправданог притиска или контроле других субјеката⁴⁶. Уколико други субјекти могу без ограничења да прикупљају и анализирају информације о здрављу, политичким ставовима, верским уверењима, сексуалном животу или другим личним својствима појединца, могућност самосталног управљања сопственим животом може бити значајно ограничена. Појединац може почети да мења своје понашање из страха да ће одређена информација бити откривена или употребљена против њега. Овај проблем је посебно изражен у дигиталном окружењу. Појединац често није у могућности да зна које се све информације о њему прикупљају, са којим другим подацима се повезују и какви се закључци на основу њих изводе.

Такође, неовлашћена обрада или откривање посебних података може нарушити достојанство лица на више начина. Откривање података о здравственом стању може довести до стигматизације, откривање верских или политичких уверења до друштвеног притиска или дискриминације, док откривање података о сексуалном животу може представљати озбиљно нарушавање интимне сфере личности. Зато се посебни подаци не штите само зато што су „тајни“, већ зато што се њиховом заштитом штити човек као носилац права. Овај аспект је нарочито важан у случајевима када лице можда формално пристаје на одређену обраду, али се поставља питање да ли је његов избор заиста слободан и информисан. У односима у којима постоји изражена неједнакост моћи, као што су односи послодавца и запосленог или пружаоца услуге и корисника, могућност формалног пристајања не значи увек и постојање стварне аутономије.

Један од најважнијих разлога за посебну заштиту ових података јесте опасност од дискриминације. Поједине категорије посебних података непосредно се односе на лична

⁴⁶ Elvira Talapina, „The Right to Informational Self-Determination: On the Edge of Public and Private“, *Law. Journal of the Higher School of Economics*, vol. 15, no. 5, 2022, стр. 24–25.

својства на основу којих је дискриминација забрањена. То се нарочито односи на расно или етничко порекло, верска уверења, политичка мишљења, здравствено стање и сексуалну оријентацију. Обрада ових података може омогућити да се лица разврставају у одређене групе и да им се, на основу такве класификације, пружа различит третман. Ризик је посебно изражен у областима као што су запошљавање, осигурање, здравствена заштита, приступ кредитима, образовање и коришћење јавних услуга. Због тога заштита посебних података има и ширу друштвену функцију. Она не штити само индивидуални интерес лица да одређена информација остане ван домашаја других субјеката, већ доприноси очувању принципа једнакости.

Посебност режима заштите посебних података огледа се и у његовој снажној превентивној функцији. Савремено право заштите података не полази само од питања шта учинити када је повреда већ настала, већ пре свега од питања како спречити да до повреде дође. Превентивни приступ је нарочито важан код посебних података јер последице њихове злоупотребе често није могуће у потпуности отклонити. Ако се, на пример, медицинска документација неовлашћено објави на интернету, накнадно брисање оригиналне објаве не гарантује да информација није копирана и даље прослеђена. Исто важи и за биометријске и генетске податке, чија се компромитација не може једноставно „поништити“.

Значај посебних података данас је додатно повећан због масовне дигитализације друштвених односа. Јавна управа, здравствени систем, банкарство, електронске комуникације, друштвене мреже и различите дигиталне услуге заснивају се на континуираној обради великих количина података. У таквом окружењу граница између информације која је непосредно откривена и информације која се може извести постаје све мање јасна. Савремени системи анализе података могу на основу великог броја наизглед неповезаних информација изводити закључке о здрављу, интересовањима, уверењима или понашању лица. Управо је зато заштита посебних података један од кључних инструмената очувања приватности у дигиталном друштву. Њена функција није само да спречи неовлашћено откривање одређене информације, већ да обезбеди да се информације о личности обрађују на начин који поштује достојанство, аутономију и равноправност појединца.

2.3 Однос између општих и посебних података о личности

У систему заштите података о личности неопходно је разликовати податке о личности који подлежу општем режиму заштите од посебних врста података о личности, за које закон предвиђа строжи режим обраде. И једна и друга категорија представљају податке који се односе на физичко лице чији је идентитет одређен или одредив, па се на њих у начелу примењују основна начела заштите података о личности. Међутим, разлика у природи, осетљивости и потенцијалним последицама њихове обраде условљава постојање додатних ограничења и гаранција у погледу посебних врста података.

Општи подаци о личности обухватају широк спектар информација које се односе на одређено или одредиво физичко лице. То могу бити, на пример, име и презиме, адреса, контакт подаци, подаци о образовању, подаци о запослењу, идентификациони подаци и други подаци који се могу повезати са конкретним лицем. Њихова обрада сама по себи није забрањена, али мора бити заснована на одговарајућем правном основу и спроведена у складу са начелима прописаним Законом о заштити података о личности.

Посебне врсте података о личности представљају ужу категорију података који због своје природе могу открити нарочито осетљиве аспекте личности. У ову категорију спадају, као што је раније наведено, подаци о расном или етничком пореклу, политичком мишљењу, верским или филозофским уверењима, чланству у синдикату, генетски подаци, биометријски подаци који се обрађују у циљу јединствене идентификације физичког лица, подаци о здравственом стању, као и подаци који се односе на сексуални живот или сексуалну оријентацију. Њихова посебност произлази из чињенице да неовлашћена обрада или откривање могу имати нарочито тешке последице по приватност, достојанство, аутономију и равноправност лица.

И општи и посебни подаци представљају податке о личности и подлежу правилима заштите. Разлика се пре свега огледа у степену ризика који њихова обрада може представљати за основна права и слободе физичког лица.

Код општих података, обрада је у начелу дозвољена уколико постоји један од законом предвиђених правних основа. Правни основ може произлазити из пристанка лица,

испуњења уговорне обавезе, испуњења законске обавезе руковаоца, заштите животних интереса, обављања послова у јавном интересу или вршења јавних овлашћења, као и из легитимног интереса руковаоца или трећег лица, када је такав основ применљив и када су испуњени законом прописани услови.

Код посебних врста података ситуација је другачија. Само постојање општег правног основа за обраду није довољно. Поред услова који се односе на законитост обраде података о личности уопште, неопходно је испунити и додатне услове предвиђене посебним режимом заштите. Управо овај „двоструки“ режим представља једну од најзначајнијих карактеристика посебних података. Стога се може рећи да однос општег и посебног режима има карактер односа правила и изузетка. Општи режим утврђује основна правила која се примењују на све податке о личности, док посебни режим додатно ограничава обраду оних података код којих постоји повећан ризик за права и слободе лица.

Најзначајнија практична разлика између општих и посебних података огледа се у условима под којима се они могу обрађивати. Код општих података руковалац мора утврдити одговарајући правни основ и обезбедити поштовање свих основних начела обраде. Код посебних врста података потребно је, поред тога, утврдити постојање посебног законског услова који оправдава њихову обраду. Ова разлика показује да пристанак лица сам по себи не представља универзално решење за обраду посебних података. Чак и када лице пристане на одређену обраду, руковалац мора водити рачуна о свим осталим условима законитости и ограничењима која произлазе из закона. Посебно је значајно да пристанак мора бити добровољан, конкретан, информисан и недвосмислен, при чему се његова ваљаност мора посматрати у контексту конкретног односа између лица чији се подаци обрађују и руковаоца.

Код обраде посебних података, осим што је неопходно испитати сврху, неопходност и сразмерност обраде, посебан акценат стављамо на принцип минимизације података. Руковалац не сме прикупљати већи обим података него што је неопходно за остваривање конкретне, легитимне сврхе. Начин обраде мора бити прилагођен и ризику који конкретна обрада носи. Код посебних података могу бити неопходне додатне техничке и

организационе мере, као што су ограничење приступа, криптографска заштита, псеудонимизација, строга контрола овлашћења, евидентирање приступа и друге мере информационе безбедности. У том смислу, правна заштита и техничка заштита не представљају одвојене механизме, већ две међусобно повезане компоненте истог система заштите.⁴⁷

Посебан правни режим не значи да је свака обрада посебних података апсолутно забрањена. Његова суштина је у томе што је полазна позиција строжа и што је круг ситуација у којима је обрада дозвољена ужи у односу на опште податке. Закон препознаје ситуације у којима је обрада посебних података неопходна ради остваривања одређених права и обавеза, заштите животно важних интереса, обављања послова од јавног интереса, пружања здравствене или социјалне заштите, као и у другим законом предвиђеним случајевима. Због тога правни режим посебних података не почива на апсолутној забрани, већ на принципу појачане правне контроле. Што је већи ризик који одређена обрада носи за права и слободе лица, то морају бити строжи услови под којима се она може спроводити.

Сагледано у целини, општи и посебни подаци о личности чине јединствен систем, али са различитим нивоима правне заштите. На опште податке примењују се основна правила законите обраде, док се код посебних врста података, поред тих правила, захтева испуњење додатних услова. Тај приступ представља израз принципа сразмерности: правна заштита мора одговарати степену ризика који одређена обрада представља за права и слободе појединца.

III НОРМАТИВНИ ОКВИР У РЕПУБЛИЦИ СРБИЈИ

Заштита посебних података о личности у правном поретку Републике Србије представља део ширег система заштите људских права, слобода и достојанства личности, чији се темељи налазе у Уставу Републике Србије, а чија се садржина и начин остваривања даље разрађују законом и другим прописима.

⁴⁷ Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године (Општа уредба о заштити података), ОЈ Л 119, 4. 5. 2016, стр. 1–88, чл. 32. ст. 1. тач. а)–г).

Нормативни оквир заштите не може се посматрати као скуп изолованих правила којима се уређује технички поступак прикупљања и обраде информација о физичком лицу. Напротив, реч је о сложенем систему правних гаранција којим се настоји успоставити равнотежа између две подједнако важне потребе савременог друштва: потребе да држава, јавне службе, привредни субјекти и друга лица могу законито да располажу информацијама неопходним за остваривање својих функција и потребе да човек задржи право да одређује границе у којима његова личност постаје предмет информисања, евидентирања, анализирања и употребе.

У том смислу, уставноправни ниво представља полазну тачку целокупног система, јер одређује вредносни оквир унутар којег се морају кретати законска правила о приватности и заштити података о личности. Нормативни оквир Републике Србије треба посматрати као хијерархијски и функционално повезан систем - од уставних јемстава људских права, преко Закона о заштити података о личности као централног прописа у овој области, до посебних правила која се примењују у управним, судским, здравственим, безбедносним, радноправним, електронским и другим областима у којима долази до обраде података о личности. Управо се у односу између ових нивоа права најбоље уочава да заштита података о личности није само питање информација, већ пре свега питање односа човека и власти, човека и институција, али и човека према сопственом идентитету и сопственом праву да одлучује шта о њему може бити познато, у коју сврху и под којим условима.

3.1 Уставна заштита права личности

Питање заштите права личности у Републици Србији мора се најпре сагледати на нивоу највишег правног акта – Устава Републике Србије. Уставна заштита представља темељ на којем почива целокупан систем заштите човекове личности, јер се њоме одређују не само појединачна права која припадају сваком човеку, већ и основне вредности које држава има обавезу да поштује, штити и унапређује. У том смислу, устав није само нормативни акт који распоређује надлежности државних органа и уређује организацију власти. Његова суштинска функција јесте да постави границе власти управо тамо где

започиње простор човекове слободе⁴⁸. Човек не постаје носилац права зато што му их држава поклања, напротив, савремена уставна држава полази од претпоставке да су одређена права неодвојива од самог постојања личности, док је задатак државе да њихово постојање призна, гарантује и обезбеди њихову делотворну заштиту⁴⁹.

Такав приступ изричито је потврђен Уставом Републике Србије. Већ у члану 1. Устав Србију одређује као државу засновану, између осталог, на владавини права, људским и мањинским правима и слободама и припадности европским принципима и вредностима. Посебно је значајна уставна одредба према којој јемства неотуђивих људских и мањинских права служе очувању људског достојанства и остварењу пуне слободе и једнакости сваког појединца у праведном, отвореном и демократском друштву заснованом на владавини права. На тај начин, достојанство, слобода и једнакост нису само опште политичке или моралне вредности, већ постају нормативни темељ тумачења читавог корпуса људских права.

Управо се у том контексту мора разумети и уставна заштита права личности. Личност човека није могуће свести на један њен аспект. Она обухвата телесни и психички интегритет, достојанство, приватност, слободу избора, идентитет, породични и интимни живот, уверења, комуникацију и, у савременом информационом друштву, податке путем којих се та личност представља и препознаје у правном и друштвеном простору. Зато заштита права личности није једно право у уском смислу, већ сложен систем међусобно повезаних гаранција.

Једно од полазних начела представља члан 18. Устава, којим је утврђено да се људска и мањинска права зајемчена Уставом непосредно примењују. Истом одредбом прописано је да се Уставом јемче и непосредно примењују људска и мањинска права зајемчена општеприхваћеним правилима међународног права, потврђеним међународним уговорима и законима, док се законом може прописати начин остваривања ових права само под условима предвиђеним Уставом. При томе, закон ни у ком случају не сме да

⁴⁸ Симоновић, И., Лазић, М., „Грађанскоправна заштита права личности“, *Зборник радова Правног факултета у Нишу*, бр. 68, 2014, стр. 281–283;

⁴⁹ Марковић, Р., *Уставно право*, Правни факултет Универзитета у Београду – Досије студио, Београд, 2015, стр. 462–463.

утиче на суштину зајемченог права. Ова уставна одредба има посебан значај за права личности, јер показује да њихова правна снага не зависи искључиво од постојања посебног закона. Закон има функцију да конкретизује начин остваривања права, да установи поступке и механизме заштите и да прецизније уреди односе између различитих субјеката, али не може да буде средство којим се суштина уставног права потискује или релативизује.

Посебно место у систему уставне заштите припада људском достојанству. Чланом 23. ст. 1. Устава Републике Србије прописано је да је људско достојанство неприкосновено и да су сви дужни да га поштују и штите, док је сваком лицу признато право на слободан развој личности, под условом да се тиме не крше права других зајемчена Уставом. Ова одредба представља један од најважнијих вредносних темеља за разумевање права личности. Достојанство је, у одређеном смислу, претпоставка свих других права. Ако се човек посматра искључиво као носилац одређених функција, података, бројева или категорија, постоји опасност да се изгуби из вида његова суштинска индивидуалност. Право, међутим, полази од супротне претпоставке, а то је да човек није предмет правног поретка, већ његов субјект.⁵⁰ Уставно схваћено достојанство тако постаје основ за идеју да човек има право да буде више од скупа података који о њему постоје у различитим регистрима, информационим системима и базама података.

Право на слободан развој личности, из члана 23. ст. 2. Устава, има нарочит значај у условима савременог информационог друштва. Личност се данас развија у окружењу у којем велики број животних активности оставља дигитални траг. Образовање, рад, здравствена заштита, коришћење јавних услуга, електронска комуникација, куповина, путовања и бројне друге активности могу бити праћене стварањем и обрадом различитих података. У таквом окружењу слобода личности више није само питање физичке слободе кретања или слободе изражавања. Она подразумева и одређени степен контроле над информационим представљањем сопствене личности. Ово је посебно видљиво код посебних категорија података. Информација о нечијем политичком уверењу може утицати на његов положај у одређеној средини, на пример, податак о здрављу може бити

⁵⁰ Ibidem.

употребљен на начин који доводи до стигматизације, податак о верским уверењима може бити основ за различито поступање, а податак о сексуалном животу може задрети у најинтимнију сферу личности. Управо зато заштита ових информација представља и заштиту простора у којем човек може слободно да обликује своју личност.

Уставна заштита права личности не исцрпљује се у заштити приватности и података. Члан 25. Устава гарантује неповредивост физичког и психичког интегритета и забрањује, између осталог, подвргавање медицинским или научним огледима без слободно датог пристанка. Ова гаранција има непосредну везу са заштитом података о здрављу и генетских података.

Посебан значај за заштиту посебних података има и уставно начело једнакости. Члан 21. Устава утврђује једнакост свих пред Уставом и законом, право на једнаку законску заштиту без дискриминације и забрањује непосредну и посредну дискриминацију по различитим основима, међу којима су изричито наведени раса, пол, национална припадност, друштвено порекло, рођење, вероисповест, политичко или друго уверење, имовно стање, култура, језик, старост и психички или физички инвалидитет. Ова одредба је од изузетног значаја за тему рада јер су поједине категорије података истовремено и потенцијални основи за дискриминаторно поступање. Информација сама по себи није нужно дискриминаторна, али њена употреба може постати средство за различито поступање према лицима.⁵¹

Уставна заштита приватне сфере личности остварује се и кроз више посебних гаранција. Чланом 40. зајемчена је неповредивост стана, док је чланом 41. гарантована неповредивост тајности писама и других средстава комуницирања.

Централно место у уставноправном систему заштите података има, као што је већ наведено, члан 42. Устава Републике Србије. Њиме је изричито зајемчена заштита података о личности, прописано да се прикупљање, држање, обрада и коришћење података уређују законом, забрањена и кажњива употреба података изван сврхе за коју су

⁵¹ Monique Mann, Tobias Matzner, „Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination“, *Big Data & Society*, 2019, Vol. 6, No. 2, стр. 1–11, посебно стр. 2–3.

прикупљени, уз уставом предвиђене изузетке, а сваком лицу признато право да буде обавештено о прикупљеним подацима о својој личности и право на судску заштиту због њихове злоупотребе.

Уставни суд је у својој пракси истакао да је заштита података о личности једно од новијих права заштите приватности које Устав гарантује и да је сврха законског уређења ове области, између осталог, обезбеђивање остваривања и заштите права на приватност и других права и слобода физичких лица.⁵² Уставни текст при томе садржи неколико кључних елемената савременог система заштите података. Прво, он успоставља гаранцију заштите података о личности. Друго, захтева да се услови њиховог прикупљања, држања, обраде и коришћења уреде законом. Треће, поставља принцип ограничења употребе података на сврху због које су прикупљени. Четврто, признаје појединцу право на информисање о подацима који су о њему прикупљени. Најзад, њиме се гарантује судска заштита у случају њихове злоупотребе. Из овога произлази да је уставна заштита података заснована на идеји контролисаног располагања информацијама о личности. Човек није потпуно господар свих информација које о њему постоје, али није ни беспомоћан пред њиховим прикупљањем и употребом.

Једно од најважнијих питања уставне заштите права личности јесте питање њиховог ограничења. Ниједно право у демократском друштву не може се посматрати као потпуно изоловано од права других лица и легитимних интереса заједнице. Међутим, могућност ограничења права не подразумева и неограничено овлашћење државе да у њихову садржину задире по сопственом нахођењу.

Члан 20. Устава прописује да се људска и мањинска права могу ограничити законом само ако ограничење допушта Устав, у сврхе ради којих га Устав допушта и у обиму неопходном да се уставна сврха ограничења задовољи у демократском друштву, без задирања у суштину зајемченог права. Истовремено, достигнути ниво људских права не може се смањивати.

⁵² Уставни суд Републике Србије, Одлука IУз-41/2010 од 30. маја 2012. године, „Службени гласник РС“, бр. 68/2012; вид. и *Билтен Уставног суда 2012–2016*, књ. I, Београд, 2018, стр. 70.

Уставна права би имала ограничену практичну вредност када не би постојали механизми њихове заштите. Због тога Устав чланом 22. гарантује свакоме право на судску заштиту када му је повређено или ускраћено неко људско или мањинско право зајемчено Уставом, као и право на уклањање последица које су повредом настале. У истом контексту предвиђена је и могућност обраћања међународним институцијама ради заштите уставом зајемчених слобода и права.

Посебну гаранцију у области података садржи управо члан 42. ст. 4. који изричито признаје право на судску заштиту због злоупотребе података о личности. Судска заштита подразумева могућност да се незаконитост обраде података подвргне независној правној контроли, да се утврди постојање повреде и да се, у зависности од конкретног правног режима, обезбеде одговарајуће последице такве повреде. У области посебних података ова гаранција добија додатни значај јер последице незаконите обраде не морају увек бити непосредно материјалне. Повреда може постојати и онда када није дошло до директног имовинског губитка, уколико је повређена приватност, достојанство, слобода избора или право лица да контролише информације о сопственој личности.

Једна од основних функција уставних права јесте постављање граница државној власти. У условима дигитализације, јавни органи све више зависе од електронских база и међусобно повезаних система у којима се обрађују подаци о грађанима. Јавна власт прикупља податке ради вођења матичних књига, пореских евиденција, здравствених и социјалних система, образовних регистара, система безбедности, статистичких истраживања и других јавних функција⁵³. Савремена држава без података практично не може да функционише, али управо зато што држава располаже великим количинама података, њена моћ над информацијама мора бити ограничена правом. У том смислу, право на заштиту података о личности има и специфичну демократску функцију. Оно успоставља однос у којем грађанин није само извор информација за државу, већ и носилац права према држави. Државни орган не располаже подацима зато што су они „његови“, већ

⁵³ Андоновић, С., Заштита података у електронској јавној управи у Републици Србији – правни аспекти, докторска дисертација, Правни факултет Универзитета у Београду, 2019., стр. 45;

зато што му је њихова обрада поверена ради конкретне, правно утемељене сврхе⁵⁴. Истовремено, заштита података не сме се схватити као препрека функционисању државе. Њена функција није да онемогући легитимну обраду, већ да је стави под услове законитости, неопходности, пропорционалности и одговорности.

Уставни систем Републике Србије не постоји у изолацији од међународног права људских права. Члан 18. Устава предвиђа непосредну примену људских и мањинских права зајемчених општеприхваћеним правилима међународног права и потврђеним међународним уговорима, док захтева и тумачење одредаба о људским и мањинским правима у корист унапређења вредности демократског друштва, сагласно важећим међународним стандардима и пракси међународних институција. У том погледу, Европска конвенција о људским правима, Повеља о основним правима Европске уније, Конвенција Савета Европе о заштити лица у односу на аутоматску обраду личних података и други релевантни међународни инструменти представљају важан део ширег нормативног контекста у којем се тумачи заштита права личности. На основу наведеног, може се са сигурношћу закључити да међународни стандарди допуњују уставни систем Републике Србије и омогућавају да се националне норме тумаче у складу са ширим развојем концепта људских права.

Из свега наведеног можемо даље извести закључак да Устав поставља темељ, али не може да одговори на сва питања која настају у сложеним процесима савремене обраде података. Он не може детаљно да уреди питање правног основа обраде, права лица на које се подаци односе, посебних услова за обраду посебних врста података, обавеза руковалаца и обрађивача, техничких и организационих мера, надзора или правних средстава. Та питања захтевају законску разраду, али законска разрада мора остати у оквирима које поставља Устав.

Из те перспективе, Закон о заштити података о личности треба посматрати као конкретизацију и разраду уставног права на заштиту података. Посебно место у том законском систему имају посебне врсте података о личности, чија осетљивост захтева

⁵⁴ Андоновић, С., Прља, Д., *Основи права заштите података о личности*, Београд, Институт за упоредно право, 2020, стр. 66–73.

строжи правни режим. Њихова заштита представља природан наставак уставног захтева да се поштују достојанство, приватност, слобода и једнакост сваког појединца. Нормативни систем тиме успоставља једну суштинску равнотежу: човек не може бити невидљив за правни и друштвени поредак, али не сме постати ни потпуно провидан пред њим⁵⁵. Између те две крајности налази се право – као граница власти, као гаранција слободе и као инструмент којим се у условима све веће информатизације друштва штити оно што је најосетљивије: сама личност човека.

3.2 Закон о заштити података о личности

Након уставноправног сагледавања заштите права личности, посебно права на заштиту података о личности, потребно је анализирати законски оквир којим се ова уставна гаранција конкретизује и претвара у систем практичних правила, обавеза и правних средстава. У том систему централно место заузима Закон о заштити података о личности („Службени гласник РС“, бр. 87/2018; у даљем тексту: ЗЗПЛ), којим се уређује право физичких лица у вези са обрадом података о личности, слободан проток таквих података, начела обраде, права лица на која се подаци односе, обавезе руковалаца и обрађивача, пренос података у друге државе и међународне организације, надзор, правна средства, одговорност и посебни случајеви обраде. Закон се примењује од 21. августа 2019. године и представља темељни пропис савременог система заштите података у Републици Србији.

Развој правне заштите података о личности у Републици Србији не може се разумети независно од ширег развоја концепта приватности, права личности и информационих технологија. Појава аутоматизованих база података, електронских регистара и могућности повезивања великог броја информација о појединцу постепено је показала да традиционални инструменти заштите приватности више нису довољни. Човек је могао да буде заштићен од неовлашћеног уласка у свој дом или од повреде тајности писама, али је истовремено могло да се догоди да се о њему прикупе стотине различитих

⁵⁵ J. C. Buitelaar, „Post-mortem privacy and informational self-determination“, *Ethics and Information Technology*, Vol. 19, 2017, стр. 129–142, нарочито стр. 134–135.

података, да се они повежу у јединствену целину и да се таква информациона слика о њему користи без његовог стварног знања⁵⁶.

У том историјском процесу значајан корак представљало је доношење Закона о заштити података о личности из 1998. године на нивоу Савезне Републике Југославије⁵⁷. Тај закон је већ тада поставио нека од темељних правила која ће касније постати трајне одреднице права заштите података: законитост прикупљања и обраде, ограничење сврхе и заштиту од неовлашћеног коришћења. Према његовим основним одредбама, лични подаци могли су се прикупљати, обрађивати и користити за сврхе утврђене законом, а за друге сврхе уз писмену сагласност грађанина. Међутим, правни, политички и технолошки контекст у којем је тај закон донет битно се разликовао од данашњег. Информациони системи почетком XXI века нису имали обим, брзину, међусобну повезаност и аналитичке могућности које имају савремени дигитални системи. Интернет је тек постепено постајао масовни комуникациони простор, док данашње технологије омогућавају готово непрекидно прикупљање и анализу података о појединцима.

Следећу важну етапу представљало је доношење Закона о заштити података о личности из 2008. године⁵⁸. Њиме је успостављен модернији институционални и нормативни оквир, а значајну улогу добио је Повереник за информације од јавног значаја и заштиту података о личности. Тај период означава прелаз од схватања заштите података као релативно уске области која се односи на евиденције и базе података ка ширем систему права, обавеза и институционалног надзора. Закон из 2008. године представљао је значајан корак у развоју националног система, али се временом показало да нормативни оквир није у потпуности одговарао динамици технолошких промена и развоју европског права.

Српски законодавац је у таквим околностима приступио изради новог законског оквира. Резултат тог процеса био је важећи Закон о заштити података о личности из 2018.

⁵⁶ Bundesverfassungsgericht, Judgment of 15 December 1983, 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, нарочито т. 150–151 образложења;

⁵⁷ Закон о заштити података о личности, „Службени лист СРЈ“, бр. 24/98 и 26/98 – исправка.

⁵⁸ Закон о заштити података о личности, „Службени гласник РС“, бр. 97/2008.

године. Његова примена започела је 21. августа 2019. године, док је престао да важи претходни Закон о заштити података о личности из 2008. године.

Историјски посматрано, може се уочити да се српско право кретало од релативно једноставног модела контроле прикупљања и коришћења података ка сложенијем моделу који обухвата цео животни циклус података. Данашњи систем више не поставља питање само да ли је неко овлашћен да прикупи податак. Постављају се и питања зашто се податак прикупља, у којем обиму, колико дуго се чува, ко му може приступити, да ли се прослеђује другом субјекту, да ли се преноси у другу државу, да ли се користи за профилисање, да ли је обрада аутоматизована и које су последице такве обраде по лице на које се подаци односе. На тај начин развој законодавства показује једну важну промену у самом разумевању података. Они више нису схваћени само као пасивни записи у административним евиденцијама, већ постају активна компонента друштвених, економских и институционалних процеса, а самим тим и предмет посебне правне заштите.

Предмет закона обухвата, пре свега, право на заштиту физичких лица у вези са обрадом података о личности и слободан проток таквих података. Поред тога, законом се уређују начела обраде, права лица на која се подаци односе, обавезе руковалаца и обрађивача, кодекси поступања, пренос података у друге државе и међународне организације, надзор, правна средства, одговорност и казне, као и посебни случајеви обраде. Закон посебно уређује и обраду коју надлежни органи врше у сврхе спречавања, истраге и откривања кривичних дела, гоњења учинилаца кривичних дела или извршења кривичних санкција, укључујући спречавање и заштиту од претњи јавној и националној безбедности. Таква структура показује да законодавац заштиту података више не посматра као једнократну правну интервенцију, већ као процес који траје од тренутка прикупљања податка до његовог брисања или другог облика престанка обраде.

Једна од суштинских карактеристика овог закона јесте то што се њиме успоставља одговорност различитих субјеката који учествују у обради. Централни појмови су руковалац и обрађивач. Руковалац одређује сврху и начин обраде, док обрађивач обрађује податке у име руковаоца и на основу његових упутстава. Ова подела одражава сложеност савремених процеса обраде, у којима лице које одређује сврху обраде често није исто лице

које непосредно управља информационим системом у којем се подаци чувају. Закон тиме успоставља ланац одговорности. Податак не губи правну заштиту само зато што је његова обрада технички поверена другом субјекту.

Формално постојање закона није довољно да би се могло говорити о потпуној заштити права. У том смислу, Повереник за информације од јавног значаја и заштиту података о личности има централну институционалну улогу. Пракса Повереника обухвата инспекцијски надзор, притужбе, жалбе и различите облике стручних мишљења, што показује да се ЗЗПЛ примењује у великом броју различитих животних ситуација. Повереник је од почетка примене ЗЗПЛ-а посебну пажњу посвећивао практичном оспособљавању руковалаца и обрађивача. Сам Повереник је указао на комплексност материје, бројне новине које је закон увео и потребу да се руковаоци и обрађивачи што боље оспособе за његову примену⁵⁹.

Једна од значајних новина савременог режима јесте јачање унутрашњих механизма одговорности руковалаца и обрађивача. У одређеним ситуацијама ЗЗПЛ предвиђа обавезу именовања лица за заштиту података о личности (енг. Data Protection Officer). Таква обавеза постоји, између осталог, када обраду врши орган власти, када основне активности руковаоца или обрађивача захтевају редован и систематски надзор великог броја лица, као и када се основне активности састоје у обради посебних врста података у великом обиму. Лице за заштиту података представља својеврсну спону између правних правила и свакодневног функционисања организације⁶⁰. Његова улога је нарочито значајна у сложеним системима у којима се велики број података обрађује континуирано.

Савремени приступ заштити података све више помера тежиште са накнадног реаговања на превенцију. Руковалац не би требало да чека да дође до повреде података како би предузео мере заштите. Мере треба да буду уграђене у сам процес обраде. То подразумева техничке и организационе мере као што су контрола приступа, ограничење овлашћења, шифровање, псеудонимизација, евидентирање приступа, раздвајање база

⁵⁹ Повереник за информације од јавног значаја и заштиту података о личности, *Извештај о раду за 2019. годину*, Београд, 2020, стр. 85;

⁶⁰ Повереник за информације од јавног значаја и заштиту података о личности, *Заштита података о личности: ставови, мишљења и пракса Повереника*, Београд, 2023, стр. 106–108.

података и периодична процена ризика. Тако се правна заштита повезује са информационом безбедношћу. Право одређује шта сме да се ради са подацима, док техничке и организационе мере треба да обезбеде да се то правило стварно спроведе⁶¹.

Иако ЗЗПЛ представља значајан искорак у развоју српског права, његова примена је показала и одређене нормативне и практичне изазове. Повереник је у новијем периоду указивао на потребу да се правни оквир даље унапређује, нарочито у условима дигитализације, развоја вештачке интелигенције, све шире употребе биометријских података и појаве нових облика обраде⁶². Ови изазови су значајни јер технологија често напредује брже од законодавства. Закон који је донет у једном технолошком тренутку мора да се примењује на системе који су неколико година касније способни да обрађују податке на начине који у време његовог доношења нису били уобичајени или нису били довољно развијени.

Важан корак у даљем развоју области представља усвајање Стратегије заштите података о личности за период од 2023. до 2030. године⁶³. Она представља покушај да се развој ове области посматра стратешки, а не само кроз појединачне измене прописа. Према доступним документима, Стратегија је усвојена 2023. године, а за њено спровођење предвиђено је доношење акционих планова. За период 2025–2027. године припремљен је посебан акциони план, уз учешће више институција и органа⁶⁴. Стратешки приступ је значајан зато што заштита података захтева координацију великог броја субјеката. Неопходно је истовремено радити на нормативном оквиру, институционалним капацитетима, едукацији, дигиталној безбедности, подизању свести грађана и развоју праксе.

Заштита података је, према томе, област у којој квалитет правног система зависи и од његове примене у свакодневном животу. Најбоља законска норма неће имати пун

⁶¹ Андоновић, С., Прља, Д., *Основи права заштите података о личности*, Београд, Институт за упоредно право, 2020, стр. 126–127;

⁶² Повереник за информације од јавног значаја и заштиту података о личности, „Састанак Радне групе за измене и допуне Закона о заштити података о личности“, 10. април 2025. године;

⁶³ Влада Републике Србије, *Стратегија заштите података о личности за период од 2023. до 2030. године*, „Службени гласник РС“, бр. 72/2023;

⁶⁴ Влада Републике Србије, *Акциони план за период од 2025. до 2027. године за спровођење Стратегије заштите података о личности за период од 2023. до 2030. године*, 2025.

ефекат ако је руковооци не разумеју, ако грађани не знају своја права или ако не постоје довољни капацитети за контролу њене примене.

Будући развој примене закона требало би посматрати и кроз промену културе заштите података. Традиционални приступ заштити података у значајној мери био је усмерен на реактивно поступање - податак се обради, догоди се повреда, лице поднесе притужбу, а надлежни орган реагује. Савремени приступ тежи супротном моделу. Ризик треба препознати пре него што се повреда догоди. То подразумева процену ризика, анализу последица обраде, увођење техничких мера, дефинисање приступа, контролу трећих лица и стално праћење усклађености.⁶⁵

Истовремено, развој дигитализације показује да законодавство у области заштите података о личности не може представљати једном заувек завршен и непроменљив систем. Развој информационих технологија, све шира употреба биометријских података, видео-надзора и система заснованих на вештачкој интелигенцији отварају нова питања која захтевају одговарајућа нормативна решења. У том смислу, чињеница да је образована посебна радна група за припрему измена и допуна Закона о заштити података о личности и да је предвиђено свеобухватније уређивање појединих савремених облика обраде података показује да постојећи правни оквир захтева даље прилагођавање изазовима дигиталног доба⁶⁶.

3.3 Улога Повереника за информације од јавног значаја и заштиту података о личности

У систему заштите података о личности није довољно постојање квалитетних законских норми. Право постаје стварно тек онда када постоји институција која његову примену надзире, тумачи, подстиче и, када је то потребно, захтева отклањање утврђених неправилности. Управо у том простору налази се Повереник за информације од јавног значаја и заштиту података о личности, као самосталан и независан државни орган надлежан за надзор над применом Закона о заштити података о личности.

⁶⁵ European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, adopted 20 October 2020, ст. 44–49;

⁶⁶ Министарство правде Републике Србије, *Полазна основа за припрему Нацрта закона о заштити података о личности*, 2025.

Повереник делује као значајан институционални механизам заштите права на заштиту података о личности, али и као саветодавни и превентивни субјект, који доприноси тумачењу и практичној примени нормативног оквира, подизању правне свести и даљем развоју ове области у Републици Србији. Важећи закон Поверенику даје широк круг надлежности и овлашћења, која обухватају надзор над применом закона, поступање по притужбама лица на која се подаци односе, давање мишљења, праћење развоја информационих и комуникационих технологија и пракси од значаја за заштиту података, израду одређених стандардних докумената, као и подстицање израде и учешће у поступку одобравања кодекса поступања⁶⁷.

Највидљивија функција Повереника јесте надзор над спровођењем Закона о заштити података о личности. Надзор има за циљ да се обезбеди да руковооци и обрађивачи испуњавају обавезе које им закон намеће и да се, у случају неправилности, предузму одговарајуће мере. Ова функција је од посебног значаја јер се заштита података не може заснивати искључиво на самоконтроли субјеката који податке обрађују. Руковалац, на пример, може имати економски, административни или други интерес да прикупи већу количину података него што је неопходно. Управо због тога мора постојати независан субјект који може да преиспита да ли је таква обрада у складу са законом.

Повереник у оквиру своје надлежности поступа на територији Републике Србије, а у вршењу својих овлашћења поступа у складу са законом којим се уређује општи управни поступак, као и сходном применом закона којим се уређује инспекцијски надзор, уколико ЗЗПЛ не предвиђа другачије. Надзорна функција, међутим, не треба да се разуме искључиво као репресивна. Њен значај огледа се и у превентивном деловању и утицају који одлуке, мишљења и пракса Повереника могу имати на уједначавање начина примене законских обавеза. Када се кроз поступање Повереника разјасни начин примене одређене законске норме или обавезе, такав став може имати значај и за друге руковооце и обрађиваче који се налазе у истој или сличној правној ситуацији.

Закон о заштити података о личности садржи велики број општих правних стандарда, а нарочито начела законитости, поштења и транспарентности, ограничења у

⁶⁷ Закон о заштити података о личности, „Службени гласник РС“, бр. 87/2018, чл. 78.

односу на сврху обраде, минимизације података, тачности, ограничења чувања, интегритета и поверљивости, као и одговорности за поступање. Ови појмови су неопходни јер омогућавају да право буде довољно флексибилно и применљиво на различите ситуације. Међутим, њихова отворена природа истовремено значи да се њихово конкретно значење развија кроз праксу. Пракса Повереника, његова мишљења, ставови, публикације, упутства и смернице омогућавају да се опште законске норме конкретизују и приближе ситуацијама у којима се примењују. Повереник на својој званичној интернет страници систематизује публикације „Ставови, мишљења и пракса Повереника“, као и различите практичне материјале намењене грађанима, руковооцима и другим субјектима, чиме се доприноси лакшем разумевању и практичној примени правила о заштити података о личности⁶⁸. Истовремено, Повереникове публикације не треба поистовећивати са законом. Оне не могу проширивати или мењати законске обавезе изван оквира који је поставио законодавац. Њихова вредност је пре свега у тумачењу, разјашњавању и практичној примени постојећих правила. Посебно место у раду Повереника заузимају практична упутства и смернице. Њихов значај је можда мање видљив од инспекцијског надзора, али је за дугорочни развој културе заштите података изузетно важан.

Посебно су значајне смернице које се односе на процену утицаја обраде на заштиту података о личности. У Публикацији бр. 8, која садржи смернице за израду процене утицаја, наглашава се потреба да се већ у фази планирања обраде идентификују правни основ, сврха, учесници у обради, а код посебних врста података и додатни услов који мора бити испуњен. Процена утицаја зато представља својеврсни мост између правне теорије и организационе праксе. Она захтева да се пре почетка ризичне обраде поставе питања који се подаци прикупљају, због чега, од кога, ко ће имати приступ, колико ће бити чувани, које су могуће последице злоупотребе и које мере могу смањити ризик. Таква логика представља помак од реактивне ка превентивној заштити.⁶⁹

⁶⁸ Повереник за информације од јавног значаја и заштиту података о личности, „Руководице – заштита података о личности“, доступно на: <https://poverenik.rs/zastita-podataka/obaveze-rukovaoca/>.

⁶⁹ Повереник за информације од јавног значаја и заштиту података о личности, *Заштита података о личности: ставови, мишљења и пракса Повереника, Публикација бр. 8 – Смернице за израду процене утицаја обраде на заштиту података о личности*; Закон о заштити података о личности, „Службени гласник РС“, бр. 87/2018, чл. 54–55;

У оквиру предмета овог рада посебну пажњу заслужује улога Повереника у заштити посебних врста података. Сам Повереник указује да посебне врсте података о личности уживају највиши степен заштите јер дубоко залазе у интиму грађана, због чега је њихова обрада, по правилу, забрањена, осим у законом прописаним и строго оправданим изузетним ситуацијама⁷⁰. Такав приступ има снажно оправдање. Код општих података, последице незаконите обраде могу бити непријатне или штетне, али код посебних података могу задрети у сам идентитет човека. Зато би улога Повереника у овој области требало да буде усмерена на неколико међусобно повезаних праваца. Прво, потребно је наставити са развојем јасних тумачења услова за обраду посебних врста података. Посебно је важно да руковооци могу јасно да разликују ситуације у којима постоји само општи правни основ од ситуација у којима мора постојати и додатни услов за обраду посебних података. Друго, потребно је наставити са развојем практичних смерница за високоризичне области: здравство, радне односе, биометрију, видео-надзор, образовање, социјалну заштиту, полицијске и безбедносне послове, научна истраживања и употребу алгоритаамских система. Треће, потребно је развијати јасне стандарде за процену неопходности и сразмерности. Чињеница да је неки податак користан не значи сама по себи да је његова обрада неопходна. Коначно, посебну пажњу треба посветити подацима који се не појављују као посебни подаци у изворном облику, али се њиховом анализом могу извести закључци о осетљивим карактеристикама појединца.

Један од најважнијих праваца будућег развоја улоге Повереника јесте јачање превентивне функције. Класичан модел заштите права често полази од претпоставке да се повреда догоди, а да онда следи реакција надлежног органа. Међутим, у области заштите података такав приступ може бити недовољан. Када се једном објаве здравствени, генетски или биометријски подаци, накнадно отклањање последица може бити практично немогуће. Зато је много ефикасније деловати пре него што до повреде дође.

У том смислу, Повереник већ располаже низом механизма који имају значајну превентивну функцију, укључујући давање мишљења, израду и објављивање смерница и

⁷⁰ Повереник за информације од јавног значаја и заштиту података о личности, „Како да остварите своја права?“, одељак „Зашто је важна заштита података о личности?“, доступно на: <https://poverenik.rs/zastita-podataka/kako-da-ostvarite-svoja-prava/>.

публикација, пружање подршке у спровођењу процене утицаја на заштиту података о личности, израду контролних листа, као и спровођење едукативних активности усмерених на подизање свести о значају заштите података о личности⁷¹. Превентивна функција је, у извесном смислу, и економски и друштвено рационалнија. Спречити незакониту обраду обично је мање сложено него накнадно отклањати њене последице. За појединца, међутим, њена вредност је још већа, јер она значи да се његово право штити пре него што буде повређено.

У краткорочном периоду, односно у наредним годинама, улога Повереника могла би се даље развијати кроз неколико практичних праваца. Први се односи на **стандардизацију праксе**. Што је више јасних упутстава, образаца, контролних листа, модела докумената и тематских смерница, то ће бити мањи простор за различито разумевање основних обавеза. Други правац представља **интензивније стручно усавршавање**. Повереник већ организује некомерцијалне обуке из области примене ЗЗПЛ-а, које држе акредитовани предавачи из Службе Повереника. Према подацима објављеним на званичној интернет страници Повереника, обуке из ове области одржаване су и током 2026. године, што потврђује да едукација и стручно усавршавање представљају редовну активност ове институције⁷². Трећи правац је **систематизација и лакша претраживост праксе**. Пракса би требало да буде тематски, хронолошки и правно систематизована, са јасним назнаком чињеничног стања, спорног питања, примењених норми и закључка. Четврти правац јесте **јачање доступности информација грађанима**. Повереник већ има посебне садржаје намењене грађанима, укључујући информације о томе како остварити права у вези са обрадом података. Овај приступ треба наставити, јер право на заштиту података не може бити делотворно ако његов носилац не зна да га има. Пети правац односи се на **посебне податке и високоризичне технологије**. Потребно је наставити са израдом тематских смерница које би организацијама омогућиле да пре почетка обраде процене ризик и утврде минималне мере заштите.

⁷¹ Повереник за информације од јавног значаја и заштиту података о личности, „Корисни савети – Заштита података о личности“.

⁷² Повереник за информације од јавног значаја и заштиту података о личности, „Обуке“, ажурирано 13. јула 2026. године; Повереник за информације од јавног значаја и заштиту података о личности, „Наставак обука из примене ЗЗПЛ за чланове Уније послодаваца Србије“, 12. мај 2026. године.

Будући развој улоге Повереника треба посматрати и у контексту раније поменуте Стратегије заштите података о личности за период 2023–2030. године. Влада Републике Србије усвојила је Стратегију 2023. године, а за њено спровођење предвиђени су акциони планови. Повереник је учествовао у јавној расправи о Стратегији, а усвојен је и Акциони план за период 2025–2027. године. Стратешки приступ је значајан јер показује да развој заштите података више не треба да буде препуштен само појединачним интервенцијама. Потребно је системски пратити развој законодавства, технологије, институционалних капацитета и јавне свести. У том процесу Повереник може имати нарочито важну улогу као институција која непосредно види проблеме у примени закона. Његова практична искуства могу представљати драгоцен извор за законодавца приликом будућих измена правног оквира.

На званичној интернет страници Повереника доступни су и материјали који обухватају смернице, препоруке и најбоље праксе Европског одбора за заштиту података, као и материјале посвећене пракси Европског суда за људска права у области заштите података о личности⁷³. Ова повезаност је посебно значајна јер право заштите података по својој природи превазилази државне границе. Подаци се преносе преко граница, чувају на серверима у различитим државама, обрађују од стране међународних компанија и користе у глобалним информационим системима. Зато ће у будућности способност Повереника да сарађује са другим надзорним органима бити све значајнија. Посебно место треба да има размена искустава, заједничко разумевање нових технологија, усаглашавање стандарда и учешће у међународним мрежама надзорних органа.

На крају, најбољи систем заштите података није онај у којем Повереник најчешће кажњава, већ онај у којем његово постојање, пракса и превентивно деловање доприносе томе да се повреде права све ређе дешавају. Смисао независног надзорног органа није само у санкцији након повреде, већ у изградњи правне и институционалне културе у којој је поштовање личности полазна претпоставка сваке обраде података. Управо у томе лежи и дугорочни значај Повереника - не само да чува постојећи стандард заштите, већ да

⁷³ Повереник за информације од јавног значаја и заштиту података о личности, „Смернице, препоруке и најбоље праксе у вези са заштитом података о личности – Европски одбор за заштиту података“ и „Водич кроз судску праксу Европског суда за људска права у вези са заштитом података на српском језику“.

доприноси његовом сталном развоју, како би право остало корак испред ризика које доноси све већа информатизација друштва.

IV ЕВРОПСКИ ПРАВНИ СТАНДАРДИ

Европски правни стандарди у области заштите података о личности представљају резултат постепеног развоја идеје да приватност и заштита личних података не могу бити посматране искључиво као питања националног права, већ као део ширег корпуса основних људских права и слобода. У праву Европске уније ова заштита има посебан значај, будући да Повеља Европске уније о основним правима одвојено гарантује право на поштовање приватног и породичног живота, дома и комуникација у члану 7, као и право на заштиту података о личности у члану 8⁷⁴. Тиме је нормативно потврђена веза између приватности и заштите података, али и њихова међусобна самосталност.

4.1 Општа уредба о заштити података (GDPR)

Општа уредба о заштити података, односно Regulation (EU) 2016/679 Европског парламента и Савета од 27. априла 2016. године, представља један од најзначајнијих нормативних подухвата у савременом европском праву приватности. Њена суштинска вредност огледа се у томе што је заштиту података поставила као сложену правну, организациону и институционалну целину, у којој се права лица чији се подаци обрађују повезују са конкретним обавезама субјеката који те податке прикупљају, чувају, користе или на други начин обрађују.

GDPR је донет 27. априла 2016. године, ступио је на снагу 24. маја 2016. године, а почео је да се примењује 25. маја 2018. године. Њиме је стављена ван снаге Директива 95/46/EЗ, која је готово две деценије представљала основни нормативни оквир Европске уније у области заштите података. За разлику од директиве, која је захтевала транспоновање у национална законодавства држава чланица, уредба је непосредно

⁷⁴ Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012, чл. 7 и 8.

применљив правни акт, чиме је настојање ка уједначавању правила добило знатно снажнији нормативни карактер⁷⁵.

Историјски развој европског права заштите података започео је знатно пре доношења GDPR-а. Важан корак представљало је усвајање Конвенције 108 из 1981. године, којом су постављени темељи европског приступа аутоматизованој обради података⁷⁶. На нивоу Европске уније овај развој настављен је Директивом 95/46/EЗ, која је настојала да истовремено обезбеди заштиту основних права и слободно кретање личних података. Технолошке и друштвене промене, међутим, постепено су показале ограничења тог оквира, што је довело до реформе европског система и коначног усвајања GDPR-а 2016. године.

Директива 95/46/EЗ од 24. октобра 1995. године представљала је први свеобухватни правни оквир Европске уније за заштиту појединаца у вези са обрадом података о личности и за слободно кретање таквих података. Њен циљ био је двострук - са једне стране, заштита основних права и слобода, а нарочито права на приватност, а са друге стране обезбеђивање слободног протока личних података између држава чланица.

Међутим, технолошке и друштвене промене које су уследиле током наредне две деценије показале су ограничења таквог нормативног оквира. Развој интернета, друштвених мрежа, електронске трговине, мобилних апликација, cloud технологија, великих скупова података, алгоритамске обраде и све интензивнијег прекограничног пословања довео је до тога да се подаци о личности више не могу посматрати само као информације садржане у ограниченим административним или пословним регистрима. Они су постали важан ресурс савремене дигиталне економије, који се користи за развој нових услуга, пословних модела и технолошких решења⁷⁷.

⁷⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016, стр. 1–88, Art. 94 and Art. 99.;

⁷⁶ М. Беванда, М. Чолаковић, „Правни оквир за заштиту особних података у праву Европске Уније“, Зборник Правног факултета Универзитета у Ријеци, 2016, стр. 126-127.;

⁷⁷ European Commission, „A European strategy for data“, 2026; European Data Protection Board, „Technology“.

Европска комисија је 2012. године предложила свеобухватну реформу европског система заштите података, са циљем да се ојачају права појединаца, поједноставе правила за прекогранично пословање и прилагоди правни оквир дигиталном добу⁷⁸. Након вишегодишњих припрема, преговора и институционалног усаглашавања, Европски парламент и Савет усвојили су 27. априла 2016. године GDPR, као део шире реформе европског права заштите података. Тако је GDPR постао резултат развојне линије која почиње заштитом приватности у условима ране аутоматизоване обраде података, наставља се кроз Конвенцију 108 и Директиву 95/46/ЕЗ, а завршава успостављањем савременог, јединственијег и знатно комплекснијег система заштите података. У том смислу, GDPR не представља потпуни прекид са претходним правним развојем, већ његову нормативну надоградњу и прилагођавање условима дигиталног друштва.

Основни циљ GDPR-а изражен је већ у самом називу Уредбе, а то је заштита физичких лица у вези са обрадом података о личности и обезбеђивање слободног кретања таквих података. Та два циља на први поглед могу деловати супротстављено. Заштита података тежи ограничавању њихове употребе, док слободан проток података подразумева њихову размену. Међутим, европски законодавац их није поставио као међусобно искључиве циљеве, већ као две стране истог правног система: подаци треба да могу слободно да циркулишу, али само у условима у којима су права и слободе физичких лица адекватно заштићени.

GDPR је структуриран тако да обухвата материјалне и територијалне претпоставке примене, основне појмове, принципе обраде, правне основе за обраду, посебне категорије података, права лица на које се подаци односе, обавезе руковалаца и обрађивача, правила о безбедности обраде, обавезу процене утицаја на заштиту података, улогу службеника за заштиту података, прекогранични пренос података, независна надзорна тела, механизме сарадње и санкције..

GDPR се примењује на обраду података о личности која се врши аутоматизовано, као и на неаутоматизовану обраду када су подаци део збирке или су намењени да буду део

⁷⁸ European Commission, *Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25 January 2012.

збирке⁷⁹. Предмет заштите су подаци који се односе на идентификовано или одредиво физичко лице. При томе се не захтева да идентификација буде могућа непосредно на основу једног податка. И више различитих информација, посматраних заједно, може омогућити идентификацију лица.

Посебно је значајна технолошка неутралност GDPR-а. Уредба се не везује за конкретну технологију која се користи у обради података, већ се примењује без обзира на технологију и начин обраде, обухватајући како аутоматизовану тако и, под прописаним условима, неаутоматизовану обраду података о личности⁸⁰. Псеудонимизовани подаци, на пример, и даље могу представљати личне податке уколико постоји могућност поновне идентификације лица. Насупрот томе, подаци који су заиста и неповратно анонимизовани више не представљају личне податке у смислу GDPR-а.

Једна од значајних карактеристика GDPR-а јесте и његов широк територијални домет. Уредба се не ограничава само на руковооце и обрађиваче који имају седиште или пословно настањене у Европској унији. Под одређеним условима, она се примењује и на субјекте који нису настањени у Унији, нарочито када нуде робу или услуге лицима која се налазе у Унији или прате њихово понашање, под условом да су испуњени критеријуми предвиђени Уредбом. На тај начин, територијални домет заштите није искључиво везан за место настањености субјекта који врши обраду, већ и за природу његових активности и њихову повезаност са лицима која се налазе у Унији⁸¹. Такво решење има посебан значај у условима глобалне дигиталне економије. Ако би примена правила зависила искључиво од територијалне локације обрађивача, заштита би лако могла бити заобиђена премештањем обраде у другу државу. GDPR настоји да спречи такву ситуацију и да заштиту повеже са стварним односом између обраде и лица чији се подаци обрађују.

Једно од најзначајнијих места у систему GDPR-а заузимају основни принципи обраде података. Они представљају нормативну основу целокупног система и истовремено

⁷⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, OJ L 119, 4 May 2016, Art. 2(1);

⁸⁰ European Commission, „Application of the GDPR“, *Data Protection*, Reference to Regulation (EU) 2016/679, Arts. 2. and 4.;

⁸¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, OJ L 119, 4 May 2016, стр. 1–88, Art. 3(2) and Recital 23.

критеријум према којем се оцењује законитост конкретне обраде. Према члану 5. GDPR-а, лични подаци се обрађују законито, поштено и транспарентно; прикупљани у одређене, изричите и легитимне сврхе; примерени, релевантни и ограничени на оно што је неопходно; тачни и ажурни; чувани само онолико дуго колико је неопходно; и обрађивани на начин који обезбеђује одговарајућу сигурност. Посебно место заузима принцип одговорности, према којем је руковалац одговоран за поштовање наведених принципа и мора бити у могућности да докаже њихово поштовање.

Принцип законитости, поштења и транспарентности подразумева да лице мора моћи да разуме шта се са његовим подацима дешава и на којој правној основи. Принцип ограничења сврхе спречава да се подаци прикупљени за једну сврху произвољно користе у друге, са њом неспојиве сврхе. Минимизација података ограничава количину података на оно што је стварно потребно за постизање конкретне сврхе. Ограничење чувања спречава неоправдано дуготрајно задржавање података, док принцип тачности захтева да се нетачни или застарели подаци исправе или уклоне.

Принцип интегритета и поверљивости уводи безбедносну димензију заштите. Он подразумева предузимање одговарајућих техничких и организационих мера ради спречавања неовлашћеног приступа, губитка, уништења, измене или неовлашћеног откривања података. На тај начин правна заштита није одвојена од информационе безбедности, већ са њом чини функционалну целину.

GDPR не заснива законитост обраде искључиво на пристанку лица. Члан 6. предвиђа више правних основа, међу којима су пристанак, неопходност за извршење уговора, испуњење правне обавезе, заштита животно важних интереса, извршење задатка у јавном интересу или вршење јавних овлашћења, као и легитимни интерес руковаоца или трећег лица, под условима прописаним Уредбом. Када је реч о посебним врстама података, испуњење једног од услова из члана 6. само по себи није довољно, већ је неопходно да буде испуњен и један од услова предвиђених чланом 9. GDPR-а, који установљава посебан режим за њихову обраду. Овакво решење има велики практични значај. Пристанак није универзална правна основа која би аутоматски легитимисала сваку обраду. Напротив,

његова ваљаност зависи од конкретних услова, а у ситуацијама у којима постоји неравнотежа између страна, његова слободност може бити посебно проблематична.

За тему овог рада од посебног је значаја поменути члан 9. GDPR-а, којим су уређене посебне категорије података о личности. Реч је о подацима који, због своје природе, могу посебно интензивно задрети у основна права и слободе појединца. У њих спадају подаци који откривају расно или етничко порекло, политичка мишљења, верска или филозофска уверења и чланство у синдикату, као и генетски подаци, биометријски подаци намењени јединственој идентификацији физичког лица, подаци о здрављу, сексуалном животу и сексуалној оријентацији.

Основно правило јесте да је обрада ових података забрањена, али GDPR истовремено предвиђа низ изузетака у којима је обрада допуштена. Међу њима се налазе изричит пристанак лица, одређене обавезе и права из области радног права, социјалне сигурности и социјалне заштите, заштита животно важних интереса, обрада од стране одређених непрофитних тела под прописаним условима, обрада података које је лице очигледно учинило јавно доступним, као и обрада неопходна за постављање, остваривање или одбрану правних захтева. Обрада је допуштена и када је неопходна због важног јавног интереса, за потребе превентивне или медицине рада, медицинске дијагнозе и пружања здравствене или социјалне заштите, као и због јавног здравља. Посебни изузеци односе се и на архивирање у јавном интересу, научно или историјско истраживање и статистичке сврхе, уз испуњење законом прописаних услова и одговарајућих мера заштите права и слобода лица.

Овде се јасно уочава специфичност нормативне конструкције GDPR-а. За обраду обичних категорија података најпре мора постојати једна од правних основа из члана 6. Код посебних категорија података, међутим, постоји додатни услов из члана 9. То значи да се законитост такве обраде не исцрпљује испуњењем опште правне основе. Потребно је истовремено испунити и посебан услов који оправдава обраду осетљиве информације. Значај оваквог приступа огледа се у томе што европски законодавац није пошао од апсолутне забране обраде осетљивих података, јер би таква забрана била неспојива са бројним легитимним друштвеним потребама. Здравствени систем, социјална заштита,

радни односи, научна истраживања и јавноздравствене политике често захтевају обраду података који припадају управо овој категорији. Стога је успостављен систем контролисаних изузетака у којем осетљивост података захтева виши степен правног оправдања и заштитних мера.

Једна од најзначајнијих карактеристика GDPR-а јесте јачање положаја лица на која се подаци односе. Уредба не третира појединца као пасивни објект обраде, већ као носиоца конкретних права која му омогућавају да буде информисан о обради својих података, да приступи подацима, захтева њихову исправку или брисање, ограничи одређене облике обраде, уложи приговор и, под прописаним условима, оствари право на преносивост података.⁸²

Право приступа има посебну важност јер представља предуслов за делотворно коришћење других права. Лице не може ефикасно захтевати исправку, брисање или ограничење обраде ако не зна који се подаци о њему обрађују.

Право на брисање, често називано и „правом на заборав“, представља један од најпознатијих института GDPR-а. Ипак, ни ово право није апсолутно. У одређеним ситуацијама интереси јавности, законске обавезе, слобода изражавања, јавни интерес у области јавног здравља или други легитимни разлози могу ограничити његову примену. На тај начин GDPR не успоставља хијерархију у којој би право на заштиту података аутоматски имало предност над свим другим правима, већ захтева њихово међусобно усклађивање.

Посебно је значајно право на преносивост података, које одражава потребу да појединац не буде трајно везан за једног пружаоца услуга због чињенице да су његови подаци похрањени у одређеном информационом систему. Ово право истовремено показује како GDPR повезује заштиту основних права са захтевима савременог дигиталног тржишта.

⁸² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, OJ L 119, 4 May 2016, стр. 1–88, Поглавље III, Чл. 12–22.

GDPR предвиђа и обавезу вођења евиденција о активностима обраде у одређеним случајевима, обавезу обавештавања о повреди података о личности, процену утицаја на заштиту података када је вероватно да ће одређена обрада произвести висок ризик по права и слободе физичких лица, као и именовање службеника за заштиту података у законом одређеним ситуацијама.

Посебно место заузима процена утицаја на заштиту података о личности. Њена суштина је превентивна – пре него што се приступи обради која може проузроковати висок ризик по права и слободе физичких лица, руковалац треба да идентификује и процени ризике повезане са планираном обрадом и да одреди мере којима се ти ризици могу умањити. Овај приступ је нарочито значајан код обраде посебних врста података о личности, јер је њихова обрада, нарочито када се врши у великом обиму, изричито препозната као ситуација која може захтевати спровођење процене утицаја на заштиту података.⁸³

GDPR посебну пажњу посвећује безбедности обраде. Према члану 32, руковалац и обрађивач дужни су да примене одговарајуће техничке и организационе мере, водећи рачуна о стању технике, трошковима примене, природи, обиму, контексту и сврси обраде, као и ризику различите вероватноће и тежине по права и слободе физичких лица. Међу мерама се наводе, између осталог, псеудонимизација и шифровање података, обезбеђивање поверљивости, интегритета, доступности и отпорности система, могућност благовременог обнављања доступности података и редовно тестирање ефикасности безбедносних мера. На овај начин GDPR уводи снажну везу између правне и техничке заштите.

Један од проблема који је дигитализација учинила посебно сложеним јесте међународни пренос података. GDPR зато успоставља посебан систем услова за пренос података у треће државе и међународне организације. Основна идеја је да чињеница да подаци напуштају територију Европске уније не сме аутоматски значити и губитак нивоа заштите који је обезбеђен европским правом. Овај део GDPR-а показује његову ширу амбицију, а то је да заштита података више није ограничена на националне границе, јер ни

⁸³ European Data Protection Board, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*, WP 248 rev.01, 4 October 2017.

савремена обрада података није ограничена националним границама. Стога се заштита мора преносити заједно са подацима, односно мора постојати правни механизам којим се обезбеђује континуитет заштите⁸⁴.

Ефикасност GDPR-а не почива само на материјалним правилима, већ и на систему независног надзора. Државе чланице имају независна надзорна тела која контролишу примену правила о заштити података, поступају по притужбама, спроводе истраге и могу изрицати корективне мере и санкције. На европском нивоу посебно место заузима Европски одбор за заштиту података, који доприноси уједначеној примени GDPR-а и развија смернице, препоруке и најбоље праксе⁸⁵. Оваква институционална структура од посебне је важности због чињенице да исти правни текст мора бити примењиван у великом броју различитих правних система. Уједначавање праксе није могуће само путем законског текста. Неопходни су стална сарадња надзорних органа, размена искустава, тумачење сложених правних питања и стварање заједничких стандарда.

За Србију је овај механизам од значаја и због чињенице да је домаћи Закон о заштити података о личности у великој мери заснован на концептима GDPR-а. Европски стандард стога не делује само као спољни нормативни узор, већ и као важан оријентир за тумачење домаћих института, нарочито у областима у којима домаћа пракса још није у потпуности развијена.

Једна од карактеристика GDPR-а која је привукла велику пажњу јесу релативно строге санкције за повреде његових правила. Предвиђене су различите корективне мере, укључујући упозорења, опомене, налоге за усклађивање обраде, ограничење или забрану обраде, као и административне новчане казне које, за одређене категорије повреда, могу достићи 20 милиона евра или, за предузећа, до 4% укупног годишњег светског промета за претходну финансијску годину, зависно од тога који је износ виши⁸⁶. Висина

⁸⁴ Вид. Court of Justice of the European Union, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18, Judgment of 16 July 2020 тач. 92–96, ECLI:EU:C:2020:559.;

⁸⁵ Уредба (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године о заштити физичких лица у односу на обраду података о личности и о слободном кретању таквих података и о стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података), OJ L 119, 4. 5. 2016, стр. 1–88, чл. 51–52, 57–58, 68 и 70, нарочито чл. 70. ст. 1. тач. е).;

⁸⁶ Ibidem, чл. 58 ст. 2 и чл. 83 ст. 5.

потенцијалних санкција има превентивну улогу, јер подстиче организације да заштиту података интегришу у своје пословање пре него што дође до повреде права. Управо зато је принцип одговорности један од темељних концепата GDPR-а. Руководилац мора бити у стању да покаже да је обрада законита, да су ризици процењени, да су предузете одговарајуће мере и да су права лица обезбеђена.

Сагледан у целини, GDPR представља прелаз са традиционалног модела заштите приватности ка комплексном систему управљања ризицима по права и слободе физичких лица. Његова новина није само у већем броју права или строжим санкцијама, већ у промени начина на који се разуме сама одговорност за обраду података. Од руковооца се више не очекује само да реагује када дође до повреде, већ да унапред препозна ризике и организује своје поступање тако да до повреде, колико је то разумно могуће, не дође.

Најзад, значај GDPR-а за Републику Србију не огледа се само у чињеници да је он један од узора домаћем Закону о заштити података о личности. Његов утицај је шири, јер он представља мерило савременог европског разумевања заштите података и важан оријентир за развој домаће правне теорије, праксе Повереника и тумачење бројних института који су у српски правни систем преузети или прилагођени под утицајем европског права.

4.2 Европска конвенција о људским правима и релевантна пракса Европског суда за људска права (ЕСЉП)

Европски систем заштите података о личности не може се у потпуности разумети без Европске конвенције за заштиту људских права и основних слобода, будући да је право на поштовање приватног и породичног живота из члана 8. Конвенције представљало један од темељних нормативних основа из којих је постепено изведена и заштита личних података. Иако Конвенција из 1950. године не садржи посебно, изричито формулисано право на заштиту података о личности, Европски суд за људска права је кроз динамичко тумачење њених одредаба развио обимну праксу којом је обухватио прикупљање, чување, употребу, откривање и размену информација које се односе на појединца. На тај начин је

члан 8. постао један од кључних инструмената европске заштите информационе приватности.

Европска конвенција за заштиту људских права и основних слобода донета је у оквиру Савета Европе у периоду непосредно након Другог светског рата. Отворена је за потписивање у Риму 4. новембра 1950. године, а ступила је на снагу 3. септембра 1953. године. Представљала је један од првих међународних правних инструмената којима су права садржана у Универзалној декларацији о људским правима добила обавезујућу уговорну снагу, уз успостављање посебног механизма међународне контроле њиховог поштовања.

Историјски значај Конвенције огледа се управо у томе што њоме заштита људских права није остала искључиво у домену унутрашњег права држава. Државе које су приступиле Конвенцији прихватиле су међународноправну обавезу да обезбеде права и слободе гарантоване њеним текстом, а истовремено су прихватиле и надзор Европског суда за људска права. Тиме је успостављен систем у којем појединац није остао без правне заштите у ситуацији када су домаћи механизми показали недостатке.

Првобитни систем контроле био је сложенији од данашњег. До ступања на снагу Протокола број 11, 1. новембра 1998. године, у систему су постојали Европска комисија за људска права, Европски суд за људска права и Комитет министара Савета Европе⁸⁷. Протоколом број 11 извршена је темељна институционална реформа: Комисија и дотадашњи Суд замењени су једним сталним Европским судом за људска права, а појединцу је омогућено да непосредно поднесе представку Суду након испуњења услова допуштености⁸⁸. Ова промена има велики значај за савремени систем заштите права. Суд више није само допунски механизам у односу на националне институције, већ стални међународни судски орган који кроз своју праксу континуирано развија стандарде заштите људских права.

⁸⁷ European Court of Human Rights, "The Situation before 1 November 1998", in *The European Court of Human Rights: Historical Background, Organisation and Procedure*;

⁸⁸ Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, restructuring the control machinery established thereby, ETS No. 155, Strasbourg, 11 May 1994, entered into force 1 November 1998.

Република Србија је приступила Конвенцији 2004. године, а Конвенција је ступила на снагу у односу на Србију 3. марта 2004. године, у време државне заједнице Србија и Црна Гора⁸⁹. Након престанка државне заједнице, Република Србија је наставила њено чланство у Савету Европе и преузете међународноправне обавезе⁹⁰.

За правни поредак Републике Србије то значи да Конвенција и пракса Европског суда за људска права представљају значајан део европског система заштите људских права са којим домаће право мора бити усклађено. У области заштите података о личности овај значај је нарочито изражен, јер се питања која су данас регулисана посебним законима често истовремено постављају и као питања заштите права на приватни живот из члана 8. Конвенције.

Члан 8. Конвенције гарантује свакоме право на поштовање приватног и породичног живота, дома и преписке. Истовремено, став 2. овог члана прописује услове под којима је могуће мешање јавне власти у наведено право. Такво мешање мора бити „у складу са законом“ и неопходно у демократском друштву ради остварења једног од легитимних циљева наведених у Конвенцији. Из наведене структуре произлази класичан европски тест оправданости мешања у право из члана 8. Најпре се испитује да ли је дошло до мешања у приватни живот, затим да ли је мешање засновано на закону, да ли има легитиман циљ и, коначно, да ли је било неопходно у демократском друштву, што укључује и испитивање сразмерности мере.

Овај модел има посебан значај за заштиту података. Наиме, обрада података од стране јавних органа често не представља класично „мешање“ у приватност у смислу физичког уласка у дом или директног надзора лица. Она може бити далеко суптилнија, тако што држава може прикупити одређене информације, унети их у базу података, чувати их годинама, повезивати их са другим информацијама или их проследити другом органу. Суд је кроз своју праксу постепено развио схватање да и такве радње могу бити обухваћене чланом 8.

⁸⁹ Council of Europe, Treaty Office, Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No. 5, Full list of signatures and ratifications — Serbia: signature 3 April 2003, ratification 3 March 2004, entry into force 3 March 2004.;

⁹⁰ ECtHR, *Matijašević v. Serbia*, no. 23037/04, Judgment of 19 September 2006, стр. 22–25.

Посебно је значајно што појам „приватног живота“ у пракси Суда није схваћен уском, формалистичком смислу. Суд га посматра као широк појам који није могуће исцрпно дефинисати и који обухвата различите аспекте личног идентитета, физичког и психичког интегритета и односа појединца са другим лицима. У савременој пракси Суд изричито потврђује да је заштита личних података гарантована правом на поштовање приватног живота из члана 8.

Један од првих значајних предмета за разумевање односа између државног надзора и члана 8. јесте *Klass and Others v. Germany*, представка број 5029/71, пресуда од 6. септембра 1978. године⁹¹. Предмет се односио на немачки систем тајног надзора поштанских и телекомуникационих комуникација ради заштите националне безбедности и демократског поретка. Значај овог предмета није само у конкретном немачком систему надзора, већ у принципу који је Суд поставио - постојање законодавства које омогућава тајне мере надзора само по себи може отворити питање заштите права из члана 8, чак и када појединац не може да докаже да је конкретно био предмет надзора. То је логична последица саме природе тајног надзора – када лице не зна да ли је надзирано, захтев да претходно докаже конкретну меру могао би право на судску заштиту учинити практично неделотворним. На тај начин Суд је већ у раној фази развоја своје праксе препознао једну од основних специфичности информационе приватности, а то је да опасност не мора да произлази само из стварног откривања информације, већ и из могућности њеног тајног прикупљања, чувања и употребе.

Следећи значајан корак представља предмет *Leander v. Sweden*, представка број 9248/81, пресуда од 26. марта 1987. године⁹². У том случају било је речи о тајном прикупљању и чувању информација о подносиоцу представке у контексту безбедносне провере. Суд је прихватио да само чување информација које се односе на приватни живот лица може представљати мешање у право из члана 8. Овај став је од изузетног значаја јер показује да се заштита не активира тек онда када се информација јавно објави. Само постојање базе података у којој се чувају личне информације може бити правно

⁹¹ European Court of Human Rights, *Klass and Others v. Germany*, no. 5029/71, judgment of 6 September 1978.;

⁹² European Court of Human Rights, *Leander v. Sweden*, no. 9248/81, judgment of 26 March 1987.;

релевантно. На тај начин постављен је један од темеља касније европске доктрине заштите личних података.

У предмету *Amann v. Switzerland*, представка број 27798/95⁹³, Велико веће је даље развило концепт информационе приватности. Предмет се односио на евидентирање информација о подносиоцу представке од стране швајцарских органа безбедности. Значај предмета огледа се у томе што је Суд наставио да шири разумевање појма приватног живота и у правцу заштите информација које државни органи прикупљају о појединцу.

За тему посебних категорија података један од најважнијих предмета у пракси ЕСЉП свакако је *S. and Marper v. the United Kingdom*, представке број 30562/04 и 30566/04, пресуда Великог већа од 4. децембра 2008. године⁹⁴. Предмет се односио на задржавање отисака прстију, узорака ћелија и ДНК профила лица која су била осумњичена, али нису осуђена. Суд је утврдио повреду члана 8. Конвенције. Посебна тежина предмета произилазила је из чињенице да се радило о биометријским и генетским информацијама, дакле информацијама које могу откривати веома дубоке аспекте идентитета појединца. Суд је указао на значај природе података, њихову способност да омогуће идентификацију и ризик који произлази из њиховог систематског чувања.

Значај ове пресуде за посебне податке је вишеструк. Прво, она потврђује да биометријски и генетски подаци захтевају нарочито пажљиву процену оправданости њихове обраде. Друго, показује да није довољно да држава покаже да подаци могу бити корисни за спречавање и откривање криминала. Неопходно је испитати и обим, трајање и услове обраде, као и постојање гаранција против злоупотребе. Треће, из предмета произлази значај принципа ограничења чувања, који ће касније бити препознат и као један од основних принципа GDPR-а.

У предмету *Roman Zakharov v. Russia*, представка број 47143/06, пресуда Великог већа од 4. децембра 2015. године⁹⁵, Суд је разматрао систем пресретања мобилних

⁹³ European Court of Human Rights, *Amann v. Switzerland* [GC], no. 27798/95, judgment of 16 February 2000.;

⁹⁴ European Court of Human Rights, *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, judgment of 4 December 2008.;

⁹⁵ European Court of Human Rights, *Roman Zakharov v. Russia* [GC], no. 47143/06, judgment of 4 December 2015.

комуникација. Предмет је посебно важан због развоја стандарда који се односе на тајни надзор и законске гаранције против произвољности. Суд је анализирао да ли национални систем садржи довољно прецизна правила која ограничавају дискреционо поступање органа власти и обезбеђују стварну контролу над мерама надзора. У контексту тајних мера, Суд је посебно заинтересован за питања која се односе на категорије лица која могу бити подвргнута надзору, природу кривичних дела или околности које могу оправдати меру, њено трајање, процедуру за одобравање, надзор над применом и могућност накнадне контроле. Значај *Zakharov*-а лежи у томе што Суд није посматрао закон само као формални основ за постојање система надзора. Захтев „у складу са законом“ подразумева и одређени квалитет закона: правила морају бити доступна, предвидљива и довољно јасна да ограниче опасност од произвољности. Овај стандард је од посебне важности за све облике обраде личних података од стране јавних органа, нарочито када се ради о великим базама података и тајним или аутоматизованим облицима обраде.

За тему овог рада нарочито је занимљив предмет *Catt v. the United Kingdom*, представка број 43514/15, пресуда од 24. јануара 2019. године⁹⁶. Подносилац је био учесник у политичким и протестним активностима, а полиција је у својој бази задржавала информације о његовој повезаности са протестним скуповима. Суд је утврдио да је задржавање таквих података представљало мешање у право на приватни живот. Посебан значај има чињеница да су информације откривале политичке активности и ставове подносиоца. Суд је у својој пракси препознао податке који откривају политичко мишљење као посебно осетљиву врсту података која захтева виши степен заштите. Овај предмет показује да се заштита приватности не односи само на информације које су традиционално сматране интимним, као што су здравље или сексуални живот. Политички ставови и учешће у јавном животу такође могу бити део заштићене сфере појединца, посебно када њихово систематско евидентирање може произвести последице по слободу политичког деловања и учешћа у демократском друштву.

Развој информационог друштва довео је и до питања да ли подаци попут IP адресе могу бити обухваћени заштитом члана 8. У предмету *Benedik v. Slovenia*, представка број

⁹⁶ European Court of Human Rights, *Catt v. the United Kingdom*, no. 43514/15, judgment of 24 January 2019.;

62357/14, пресуда од 24. априла 2018. године⁹⁷, Суд је разматрао питање приступа полиције подацима повезаним са динамичком IP адресом коришћеном приликом приступа интернет садржају. Предмет је значајан јер показује да дигитални идентификатори не могу бити посматрани као правно неутрални технички подаци. Када одређена информација омогућава повезивање интернет активности са конкретним физичким лицем, она може задобити карактер информације релевантне за приватни живот. У овом предмету Суд је посебно разматрао очекивање приватности у дигиталном окружењу и услове под којима државни органи могу приступити информацијама које омогућавају идентификацију корисника. Овај предмет је значајан и због тога што показује да се Конвенција тумачи у светлу технолошких промена.

Један од најзначајнијих савремених предмета јесте *Big Brother Watch and Others v. the United Kingdom*, представке број 58170/13, 62322/14 и 24969/15, пресуда Великог већа од 25. маја 2021. године⁹⁸. Предмет је обухватао различите режиме електронског надзора, укључујући масовно пресретање комуникација, прибављање комуникационих података од пружалаца комуникационих услуга и размену пресретнутог материјала са страним државама и обавештајним службама. Суд је утврдио повреду члана 8. у погледу режима масовног пресретања комуникација и режима прибављања комуникационих података од пружалаца услуга. Такође, прихватио је да савремене безбедносне претње могу довести до потребе за коришћењем сложених система надзора, али је нагласио значај одговарајућих гаранција против злоупотребе. Овај предмет је од посебног значаја јер показује како се класични стандард из члана 8. примењује на савремене системе који обрађују огромне количине података. Питање више није само да ли држава прислушкује конкретну особу, већ како је читав систем постављен, ко може да покрене обраду, који су услови за приступ подацима, ко врши надзор, колико се подаци чувају и које постоје гаранције за њихово коришћење. Таква логика непосредно је повезана са савременим концептом заштите

⁹⁷ European Court of Human Rights, *Benedik v. Slovenia*, no. 62357/14, judgment of 24 April 2018.;

⁹⁸ European Court of Human Rights, *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13, 62322/14 and 24969/15, judgment of 25 May 2021.

података заснованим на ризику. Што је већи обим обраде и што је дубљи могући утицај на приватност, то су значајније правне, институционалне и техничке гаранције.

Из наведене праксе може се уочити да Европски суд за људска права заштиту података о личности не гради кроз један изоловани институт, већ кроз шири концепт права на приватни живот. То значи да се заштита података у систему Конвенције активира у ситуацијама у којима обрада информација о појединцу задире у сферу његовог приватног живота.

За Републику Србију значај праксе Европског суда није само теоријски. Србија је обавезана Конвенцијом, а Суд у Стразбуру представља међународни механизам контроле поштовања права гарантованих Конвенцијом. Због тога домаћи органи, а нарочито судови, приликом тумачења права која се поклапају са правима из Конвенције морају водити рачуна о стандардима који су развијени у пракси Суда.

Најзад, развој праксе ЕСЉП потврђује да заштита приватности није статична категорија. Конвенција је управо захваљујући еволутивном тумачењу успела да остане релевантан инструмент у условима које њени творци нису могли предвидети.

4.3 Хармонизација српског законодавства са европским стандардима

Хармонизација права Републике Србије са европским стандардима у области заштите података о личности представља процес који је током последњих деценија прошао кроз значајне нормативне промене, али који још увек није окончан. Његова суштина, при томе, не може се свести на просто преузимање европских правних решења у домаће прописе.

Посебан изазов представља чињеница да технолошки развој често напредује брже од способности правног система да на време препозна и уреди нове облике обраде података, због чега се јаз између нормативне заштите и њене практичне примене може постепено продубљивати⁹⁹. У таквим околностима посебне врсте података о личности

⁹⁹ European Data Protection Supervisor (EDPS), *Review of the EDPS mandate, 2015–2019*, одељак „Data protection goes digital“.

добијају додатну тежину, јер се њиховом дигиталном обрадом могу створити дубоки и трајни увиди у идентитет, здравље, уверења, понашање и приватни живот појединца. Стога се изазови примене не односе само на поштовање формалних законских обавеза, већ и на обезбеђивање стварне контроле лица над сопственим подацима, спречавање неовлашћеног приступа и секундарне употребе, обезбеђивање транспарентности и одговорности, адекватну примену техничких и организационих мера, као и на способност институција и руковалаца да правне принципе преведу у делотворне поступке и технологије.

Један од најважнијих корака у том правцу представља доношење Закона о заштити података о личности од 2018. године, којим је домаћи нормативни оквир у значајној мери приближен стандардима Опште уредбе о заштити података – GDPR. Закон је преузео читав низ основних института савременог европског права: принципе обраде, права лица на које се подаци односе, положај руковоца и обрађивача, процену утицаја на заштиту података, службеника за заштиту података, обавештавање о повреди података, посебне категорије података, правила о преносу података и систем надзора и корективних мера. Поред тога, Србија је уговорно повезана са европским системом заштите података и путем Конвенције Савета Европе о заштити лица у односу на аутоматску обраду личних података и њеног модернизованог протокола.

У нормативном смислу, стога, може се констатовати да је учињен велики корак. Домаће законодавство више не припада моделу у којем је заштита података схваћена као споредно административно питање, већ је постављена као систем заштите основног права појединца. Посебно је значајно што је домаћи закон прихватио европску концепцију према којој се законитост обраде не исцрпљује у постојању формалног правног основа, већ захтева поштовање читавог низа принципа, укључујући законитост, транспарентност, ограничење сврхе, минимизацију, тачност, ограничење чувања, интегритет и поверљивост.

Ипак, управо ту почиње разлика између **нормативне хармонизације и стварне хармонизације**. Није довољно да домаћи закон садржи европски стандард; потребно је да се тај стандард доследно примењује у свим областима у којима се лични подаци обрађују. Посебан проблем представља чињеница да, према извештају Повереника, процес

усклађивања других закона и прописа са Законом о заштити података о личности није био у потпуности окончан у предвиђеном року, који је, у складу са чланом 100. Закона, истекао крајем 2020. године¹⁰⁰. Повереник је указао да поједини секторски прописи и даље садрже решења која нису у потпуности усклађена са савременим системом заштите података, због чега су потребне измене појединих прописа или доношење нових. Није неопходно да сваки домаћи пропис буде дословна копија GDPR-а, нити је то правно ни практично могуће. Европски стандарди остављају простор за национална правила тамо где је то оправдано природом одређене области. Оно што, међутим, јесте неопходно, јесте да сваки посебан режим обраде буде заснован на јасној сврси, одговарајућем правном основу, неопходности и сразмерности, уз обезбеђивање делотворних права лица и одговарајућих механизма надзора.

Посебно је значајно што је Република Србија, по ранијој напмени, у августу 2023. године усвојила Стратегију заштите података о личности за период 2023–2030. године, а затим и Акциони план за период 2025–2027. године. Стратегија је усмерена управо ка даљем усклађивању правног оквира са европским правилима и стандардима, јачању права грађана и институционалних капацитета и унапређењу целокупног система заштите. Акциони план је усвојен 2025. године и предвиђа конкретне активности за спровођење Стратегије.

Значајан корак у даљем унапређивању нормативног оквира представља чињеница да је у јануару 2025. године формирана Посебна радна група за припрему измена и допуна Закона о заштити података о личности¹⁰¹. Њен задатак је, између осталог, припрема радне верзије измена закона. Тако је процес хармонизације ушао у нову фазу: након доношења основног нормативног оквира, пажња се све више усмерава ка његовом усавршавању и отклањању недостатака уочених у примени.

У будућем развоју посебну пажњу треба посветити посебним категоријама података о личности. Њихова осетљивост захтева да законодавац избегава сувише широке и

¹⁰⁰ 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 2020. годину*, Београд, март 2021, стр. 5.

¹⁰¹ 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 2025. годину*, Београд, 2026, стр. 90.

неодређене формулације којима се омогућава обрада здравствених, генетских, биометријских, политичких или других осетљивих података без јасних ограничења. У том погледу европски стандард није само захтев да постоји правни основ, већ и да се може објаснити зашто је обрада неопходна, у којој мери, у коју сврху, колико дуго и уз које гаранције.

Истовремено, хармонизација мора бити праћена **јачањем институционалних капацитета Повереника**. Независност надзорног органа има смисла само ако је праћена одговарајућим кадровским, техничким и финансијским ресурсима. Повереник већ спроводи активности усмерене на системско унапређење заштите, укључујући иницијативе за измену закона, давање мишљења на прописе и едукацију субјеката који обрађују податке. Даљи развој ових активности требало би да буде усмерен ка још већој превентивној улози, нарочито у областима у којима се обрађују велике количине посебних категорија података.

Најзад, најважнија будућа промена можда није у доношењу још једног прописа, већ у развоју **културе заштите података**. Европски стандард се не исцрпљује у тексту закона. Он подразумева да државни орган службени податак не доживљава као нешто што му припада без ограничења, да привредни субјект не посматра личне податке искључиво као пословни ресурс, а да грађанин зна да има право да пита шта се о њему прикупља, зашто се прикупља и колико дуго се чува. Само у таквом окружењу правни принципи постају стварна права.¹⁰²

Стога се досадашњи пут Републике Србије може описати као **значајно нормативно приближавање европском моделу, али још недовршена практична хармонизација**. Оно што је било неопходно на нивоу основног законодавства у великој мери је учињено доношењем Закона о заштити података о личности из 2018. године и прихватањем европских и међународних стандарда. Оно што није неопходно јесте механичко преписивање сваког европског правила у домаће законодавство. Оно што, међутим, јесте неопходно и што не би требало одлагати јесте усклађивање преосталих секторских

¹⁰² European Data Protection Supervisor (EDPS), „The Accountability Initiative“, 7 јун 2016.

прописа, јачање институционалних капацитета, уједначавање праксе и прилагођавање правног система новим облицима обраде података.

V ИЗАЗОВИ И ПРАКТИЧНИ ПРОБЛЕМИ У ПРИМЕНИ

Поред нормативног успостављања система заштите података о личности, његова стварна делотворност зависи од начина на који се правне норме примењују у условима савременог друштва, које карактеришу убрзана дигитализација, развој информационих и комуникационих технологија, масовна обрада података, међусобно повезивање база података, употреба биометријских система, профилисање, аутоматизовано доношење одлука и све шира примена вештачке интелигенције. Посебан изазов представља чињеница да технолошки развој често напредује брже од способности правног система да на време препозна и уреди нове облике обраде података, због чега се јаз између нормативне заштите и њене практичне примене може постепено продубљивати. Стога се изазови примене не односе само на поштовање формалних законских обавеза, већ и на обезбеђивање стварне контроле лица над сопственим подацима, спречавање неовлашћеног приступа и секундарне употребе, обезбеђивање транспарентности и одговорности, адекватну примену техничких и организационих мера, као и на способност институција и руковалаца да правне принципе преведу у делотворне поступке и технологије. У том смислу, савремена заштита података о личности све више постаје питање истовремене правне, институционалне и технолошке одговорности.

5.1 Технолошки развој и дигитализација као изазов

Савремено друштво све се теже може замислити изван дигиталног простора. Готово свака област човековог живота данас оставља за собом одређени дигитални траг: комуникација, образовање, здравствена заштита, радни однос, коришћење финансијских услуга, кретање, куповина, коришћење електронских уређаја, приступ јавним услугама, па чак и најразличитији облици друштвене интеракције. Оно што је некада било распршено, привремено и тешко доступно, савремена технологија претвара у податак који се може забележити, сачувати, повезати са другим подацима и поново употребити. На тај начин

дигитализација није донела само нове техничке могућности, већ је постепено променила и саму природу информације као друштвене и правне категорије.

У традиционалном друштвеном окружењу информација о појединцу најчешће је имала ограничен домет. Њено ширење било је условљено физичком доступношћу документа, непосредношћу комуникације и временом потребним за њено преношење. У дигиталном окружењу такве границе готово да више не постоје. Једном унет податак може се готово тренутно умножити, пренети на велики број система, обрадити аутоматизованим средствима и довести у везу са другим информацијама које наизглед немају никакву непосредну везу са првобитном сврхом обраде. Управо у томе лежи један од основних изазова савремене заштите података, јер проблем више није само у томе који се податак прикупља, већ и у томе са којим се другим подацима он може повезати, шта се из такве повезаности може закључити и какве последице такав закључак може произвести.

Ова промена посебно је значајна када је реч о посебним врстама података о личности. Информација о здравственом стању, генетским карактеристикама, биометријским обележјима, верским или политичким уверењима, припадности синдикату или сексуалном животу и оријентацији већ сама по себи представља податак чија злоупотреба може озбиљно угрозити приватност и достојанство појединца. Међутим, у дигиталном окружењу ризик се не исцрпљује у њиховом непосредном откривању. Савремени системи могу из великог броја наизглед неповезаних информација извести нове закључке о појединцу, при чему лице чији се подаци обрађују понекад није ни свесно да је одређена особина постала предмет обраде. Управо зато савремена заштита података све више мора да обухвата не само податке које је лице непосредно саопштило, већ и ризике који настају њиховим комбиновањем, анализом и извођењем нових информација.

У том смислу, једно од суштинских обележја дигитализације јесте **масовност обраде података**. Велики подаци, односно Big Data, омогућавају обраду количина информација које би у традиционалним условима биле практично неупотребљиве. Вредност таквих система управо се често заснива на способности да се велики број појединачних информација повеже и анализира као целина. Овај проблем је посебно

изражен код посебних врста података, јер њихово повезивање са другим информацијама може омогућити креирање изузетно детаљних профила личности¹⁰³.

Дигитализација, према томе, доводи у питање и традиционално схватање принципа ограничења сврхе. Ако се подаци прикупљају за једну, унапред одређену сврху, а потом даље обрађују или преносе у друге информационе системе, јавља се питање да ли је таква даља обрада компатибилна са првобитном сврхом њиховог прикупљања¹⁰⁴. На пример, податак који је првобитно прикупљен ради пружања здравствене услуге може у одређеним околностима постати део статистичке, истраживачке, административне или аналитичке обраде. Сама чињеница да технологија омогућава такву употребу не значи да је она аутоматски и правно допуштена. Напротив, што су могућности технологије веће, то је значај правних ограничења већи, јер се правом мора одредити граница између онога што је технички могуће и онога што је правно и друштвено прихватљиво.

Посебан проблем представљају **биометријски подаци**. Савремени системи препознавања лица, гласа, ириса, отиска прста и других јединствених карактеристика човека омогућавају идентификацију појединца са високим степеном аутоматизације. За разлику од лозинке или другог средства које се може променити, биометријски подаци су непосредно повезани са карактеристикама самог појединца, због чега њихов губитак, неовлашћено откривање или злоупотреба могу имати нарочито озбиљне и дуготрајне последице по приватност и идентитет лица¹⁰⁵. Ако лозинка буде компромитована, она се може променити; човек, међутим, не може променити сопствено лице, отисак прста или основну генетску структуру. Ова особеност додатно оправдава појачану правну заштиту биометријских и генетских података. Проблем постаје још сложенији када се биометријска технологија повезује са системима за видео-надзор, мобилним уређајима, јавним просторима и другим дигиталним инфраструктурама. Тада више није реч само о идентификацији једног лица у конкретној ситуацији, већ о могућности континуираног

¹⁰³ European Data Protection Supervisor, *Opinion 7/2015: Meeting the challenges of big data – A call for transparency, user control, data protection by design and accountability*, 19 November 2015, стр. 5–6 и 8–10.;

¹⁰⁴ Вид. Суд правде Европске уније, *ND and Others v. Digi Communications NV*, C-77/21, 20. октобар 2022, т. 25–27, 45;

¹⁰⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council, чл. 4 тач. 14 и чл. 9; European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement – Version 2.0*, 17 May 2023, т. 12–15, 21–23.

праћења и повезивања идентитета са временом, местом и понашањем појединца. Европски одбор за заштиту података посебно указује на значај савремених технологија, укључујући биометријско препознавање и технологије праћења, које, иако доносе бројне користи и нове могућности, истовремено стварају нове ризике и изазове за заштиту приватности, као и заштиту и безбедност личних података¹⁰⁶.

Нарочито је значајно питање **извода и закључака који се могу извести из података**. Дигитални систем не мора добити податак у облику у којем се тај податак непосредно препознаје као осетљив. Одређене информације могу, у комбинацији са другим подацима, омогућити закључивање о здравственом стању, политичком уверењу, верској припадности или другим карактеристикама личности. Савремено право заштите података зато не може остати усмерено искључиво на питање шта је лице изричито саопштило, већ мора узимати у обзир и начине на које технологија омогућава да се о њему сазна нешто што оно никада није непосредно открило.

С тим у вези, посебно значајан постаје институт **профилисања**. Аутоматизована анализа понашања може омогућити креирање профила који садрже претпоставке о интересовањима, навикама, способностима или особинама појединца. Иако такве информације понекад нису тачне, њихов значај може бити велики ако се користе приликом доношења одлука које производе правне или друге значајне последице. Опасност се додатно повећава када се профилисање врши на основу података који непосредно или посредно откривају посебне врсте података. На тај начин технолошки систем може, чак и без намере да „обрађује“ одређену осетљиву особину, доћи до закључка који задире у најдубље сфере приватности појединца.¹⁰⁷

Зато дигитализација захтева и другачије разумевање принципа минимизације података. Традиционални приступ могао је почивати на питању да ли је одређени податак потребан за конкретну административну или пословну радњу. У савременом дигиталном

¹⁰⁶ European Data Protection Board, *Technology*, EDPB, „AI and Technology“, доступно на: https://www.edpb.europa.eu/topics/ai-and-technology_en;

¹⁰⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council, чл. 4 тач. 4, чл. 9 и чл. 22; Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251rev.01, 6 February 2018, стр. 5–6, 15; European Data Protection Board, *Guidelines 08/2020 on the targeting of social media users*, Version 2.0, 13 April 2021, т. 121.

окружењу потребно је поставити и додатна питања: да ли је неопходно прикупљати управо такав обим података, колико дуго их је потребно чувати, да ли се могу користити мање инвазивна средства, да ли је могуће постићи исти циљ употребом анонимизованих или псеудонимизованих података и шта се може догодити ако се различите базе података повежу.

У том погледу посебан значај има концепт **заштите података по дизајну и по подразумеваним поставкама**. Суштина овог приступа јесте у томе да заштита приватности не буде накнадно „додата“ систему када је он већ изграђен, већ да буде један од његових почетних конструктивних елемената¹⁰⁸. ENISA у свом извештају о Data Protection Engineering указује на значај разматрања техничких и организационих мера заштите података већ приликом пројектовања система. Такав приступ омогућава да се принципи заштите података не задрже само на нивоу правних захтева, већ да се њихова примена обезбеди и кроз избор, имплементацију и конфигурисање одговарајућих технологија и мера у самој архитектури система.¹⁰⁹ Овакав приступ има посебну вредност код посебних врста података. Ако је систем од самог почетка конципиран тако да прикупља минималан број података, ограничава приступ, раздваја идентификационе податке од садржинских информација, примењује псеудонимизацију и шифровање, бележи приступе и омогућава контролу над периодом чувања, ризик од повреде права може бити значајно смањен. Супротно томе, ако је систем изграђен тако да подразумева широку доступност података, неограничено чување и вишеструку секундарну употребу, накнадне правне или организационе интервенције често не могу у потпуности отклонити већ створене ризике.

Управо се овде показује значај повезивања правних и техничких стандарда. Захтеви поверљивости, интегритета, доступности, контроле приступа и управљања ризиком морају бити подржани одговарајућом архитектуром информационог и мрежног система. Посебно код посебних врста података, безбедност мрежа и комуникационих система представља саставни део практичне заштите права лица, јер од начина пројектовања, управљања и

¹⁰⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council, чл. 25; European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, Version 2.0, adopted on 20 October 2020, т. 44–49.;

¹⁰⁹ ENISA, *Data Protection Engineering*, January 2022, стр. 6 и 34.

надзора мрежне инфраструктуре зависи и степен изложености података неовлашћеном приступу.¹¹⁰

ISO/IEC 27001, NIST стандарди и ENISA смернице не представљају замену за правне норме, али омогућавају да се захтеви поверљивости, интегритета, доступности, контроле приступа и управљања ризиком преведу у конкретне механизме информационе безбедности¹¹¹. Посебно је значајан принцип најмањих привилегија, према којем приступ подацима треба да буде ограничен на онај обим који је неопходан за обављање конкретне функције. Код посебних врста података овај принцип добија додатну тежину, јер сваки непотребан приступ не представља само технички безбедносни ризик, већ потенцијално и повреду основних права личности.

Коначно, савремени систем заштите посебних врста података мора настојати да успостави равнотежу између две наизглед супротстављене потребе: потребе друштва да користи предности дигиталних технологија и потребе појединца да задржи стварну контролу над информацијама које се тичу његовог идентитета, достојанства и приватности. Та равнотежа не може бити једном заувек успостављена, јер се са сваком новом технологијом поново поставља питање граница дозвољене обраде. Управо зато заштита података у дигиталном добу представља процес непрекидног прилагођавања права технологији, али и технологије праву.

5.2 Злоупотреба података у пракси

Иако је нормативни оквир заштите података о личности заснован на бројним принципима, ограничењима и механизмима контроле, стварна вредност тих правила најочигледније се испољава тек у тренутку када се постави питање њихове примене у конкретном случају. Управо се на практичном плану показује да повреда права на заштиту података не настаје искључиво као последица намерне злоупотребе или свесног незаконитог поступања. Она може бити последица непажње, недовољно јасних процедура, прекомерног приступа подацима, неадекватне техничке заштите, погрешне процене

¹¹⁰ ISO/IEC 27033-1:2015, Information technology — Security techniques — Network security — Part 1: Overview and concepts;

¹¹¹ ISO/IEC 27001:2013, A.10; NIST, SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, Gaithersburg, 2020; ENISA, Risk Management Standards, 2022.

ризика, грешке запосленог или непостојања јасне границе између дозвољене и недозвољене употребе података. Посебан проблем настаје онда када су предмет таквог поступања посебне врсте података о личности, јер последице њиховог откривања или неовлашћене употребе могу далеко превазићи уобичајени ризик по приватност.

У том смислу, злоупотребу података не треба схватити искључиво као ситуацију у којој неко намерно користи туђе податке ради стицања користи или наношења штете. Много шири појам представљају све ситуације у којима се подаци обрађују супротно принципима законитости, поштења и транспарентности, изван утврђене сврхе, у већем обиму него што је неопходно, без одговарајућег правног основа или без адекватних техничких и организационих мера¹¹².

Посебна тежина овог проблема произлази из чињенице да се једном откривени подаци веома тешко могу „вратити“ у сферу приватности. Новчана накнада или административна санкција могу представљати правни одговор на повреду, али не могу у потпуности поништити чињеницу да је одређена информација већ постала доступна неовлашћеном лицу. То је нарочито видљиво код података о здрављу, генетских и биометријских података, као и података који откривају политичка или верска уверења, сексуални живот или оријентацију. Код таквих података сама чињеница откривања може променити положај појединца у друштву, изложити га стигматизацији или дискриминацији и створити последице које се не могу једноставно отклонити брисањем податка из конкретне базе.

Један од најчешћих облика злоупотребе у пракси јесте **неовлашћени приступ подацима**. Посебно је ризичан у системима у којима велики број запослених или других корисника има приступ истој бази података, јер повећање броја корисника истовремено повећава потребу за јасним разграничењем приступних овлашћења и омогућити приступ само оним подацима и ресурсима који су неопходни за обављање конкретних задатака¹¹³. Принцип ограничења приступа захтева да сваки корисник има само она овлашћења која су

¹¹² Андоновић, С., Прља, Д., *Основи права заштите података о личности*, Београд, Институт за упоредно право, 2020, стр. 66–68, 72–73; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, чл. 5 ст. 1 и чл. 6.

¹¹³ NIST, *SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations*, Gaithersburg, 2020, стр. 36, контрола AC-6 (Least Privilege);

му неопходна за обављање конкретних послова. Уколико се та граница не успостави, могућност злоупотребе постаје системски ризик, а не само индивидуални пропуст запосленог. Нарочито је значајан пример здравственог сектора, у којем се обрађује велики број посебно заштићених података. Савремени здравствени информациони системи повезују медицинску документацију, лабораторијске резултате, дијагнозе, терапије, снимке, податке о осигурању и друге информације. Предност такве дигитализације јесте у бржем и ефикаснијем пружању здравствених услуга, али њена друга страна представља чињеница да један безбедносни пропуст може омогућити приступ огромном броју података.

То потврђује и новија пракса надзорних органа у Европи. У септембру 2026. године Европски одбор за заштиту података објавио је одлуку француског надзорног органа CNIL у предмету који се односио на једну приватну болницу¹¹⁴. Нападач је успео да приступи електронском систему који је садржао податке више од 524.000 пацијената, при чему су међу подацима били и подаци о здрављу. Утврђено је, између осталог, да спољни приступ систему није био довољно заштићен, да нису били примењени VPN и вишефакторска аутентификација, као и да контрола приступа није била ограничена на здравствене раднике који су стварно учествовали у лечењу конкретног пацијента. Нападач је, користећи један кориснички налог, могао да приступи подацима великог броја пацијената, а ненормална активност није била благовремено откривена. Надзорни орган је због утврђених пропуста изрекао новчану казну од 500.000 евра.

Други случај неовлашћеног приступа подацима из здравственог сектора односи се на пољску јавну здравствену установу SPZOZ у Пајенчну, којој је 2024. године пољски надзорни орган изрекао новчану казну након ransomware напада. Напад је довео до губитка приступа подацима о око 30.000 пацијената и више од 1.000 запослених. У компромитованом систему налазиле су се различите категорије података, укључујући идентификационе, финансијске, приступне и здравствене податке. Посебно је значајно што је надзорни орган утврдио да пре инцидента није била спроведена и документована

¹¹⁴ CNIL, Délibération de la formation restreinte n° SAN-2026-009 du 21 juillet 2026 concernant la société HÔPITAL PRIVÉ DE LA LOIRE; European Data Protection Board, “Health data breach: the CNIL fined Hôpital Privé de la Loire 500 000 EUR”, 9 September 2026.

одговарајућа анализа ризика за податке о личности. Због тога установа није могла на адекватан начин да процени претње и примени одговарајуће техничке и организационе мере заштите. Пољски надзорни орган је због утврђених повреда одредаба GDPR-а изрекао новчану казну у износу од 9.300 евра и наложио спровођење додатних мера заштите.¹¹⁵

Поред сајбер-напада, значајан број повреда настаје и услед **људске грешке**. Погрешно послат електронски документ, погрешно адресирана електронска пошта, ненамерно откривање података трећем лицу или приступ подацима који није неопходан за конкретан радни задатак могу имати исте правне последице као и сложенији технички напад.

Злоупотреба може настати и онда када подаци нису прибављени незаконито, већ се **законито прикупљени подаци касније употребе за другу сврху**. Ова појава је нарочито значајна у условима дигитализације, јер подаци који су једном смештени у информациони систем постају технички доступни за бројне потенцијалне употребе. Управо зато принцип ограничења сврхе има суштинску улогу у спречавању постепеног ширења обраде. Чињеница да организација законито поседује одређени податак не даје јој неограничено право да га користи у било којој каснијој ситуацији.

На крају, пракса показује да највећи проблем није увек у непостојању правних правила, већ у њиховом недовољно доследном претварању у свакодневну праксу. Зато није довољно само прописати техничке и организационе мере, већ је потребно периодично проверавати њихову стварну ефикасност кроз процену безбедности, тестирање, идентификовање рањивости и отклањање уочених недостатака. Принцип одговорности зато захтева не само постојање мера заштите, већ и проверу да ли оне заиста функционишу у условима конкретног информационог система.¹¹⁶

Посебне врсте података о личности у том смислу представљају својеврсну границу одговорности система заштите података. Тамо где се обрађују информације које задиру у

¹¹⁵ Prezes Urzędu Ochrony Danych Osobowych, decyzja DKN.5131.57.2022, 13. jun 2024; European Data Protection Board, “Polish SA: fine of 9 300 € for Independent Public Health Care Centre after hacker attack”, 28 November 2024.

¹¹⁶ Scarfone, K. A., Souppaya, M. P., Cody, A., Orebaugh, A., NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, NIST, 2008.

најинтимније сфере човековог живота, није довољно питати да ли је податак формално заштићен. Потребно је питати да ли је његова заштита стварна, да ли постоји контрола над приступом, да ли се може спречити његова секундарна употреба и да ли систем може благовремено да препозна и ограничи последице повреде. Заштита података, стога, своју коначну вредност не доказује бројем законских одредаба, већ тренутком у којем те одредбе треба да заштите конкретног човека. Управо у томе се и огледа разлика између права које само прописује заштиту и права које ту заштиту заиста остварује.

5.3 Баланс између јавног интереса и права личности

Право на заштиту података о личности, као и право на приватност, није право које постоји у потпуној изолацији од других права и интереса друштва. Живот у организованој заједници нужно подразумева ситуације у којима држава, јавне установе или друга овлашћена лица морају располагати одређеним подацима о грађанима како би обављали послове од значаја за целу заједницу. Здравствена заштита, спречавање и откривање кривичних дела, заштита јавне безбедности, остваривање права из социјалне заштите, функционисање правосуђа или заштита живота и здравља људи само су неки од примера у којима потпуно искључивање обраде личних података не би било могуће, а понекад ни разумно. Због тога савремено право не поставља питање тако да једна страна увек мора победити другу. Његов задатак је да успостави границу између онога што је за остваривање јавног интереса заиста потребно и онога што би представљало неоправдано задирање у права личности.

Јавни интерес, према томе, представља легитиман разлог за одређену обраду података, али сам по себи није неограничено овлашћење. Посебно се овај однос испољава у области приступа информацијама од јавног значаја. Остваривање права јавности да буде информисана не искључује обавезу да се заштите подаци о личности који се налазе у таквим информацијама. Због тога се приступ информацијама мора остваривати уз истовремено поштовање ограничења која произлазе из права на приватност и заштиту података о личности¹¹⁷.

¹¹⁷ Закон о слободном приступу информацијама од јавног значаја, „Службени гласник РС“, бр. 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021;

Најједноставније речено, **јавни интерес може оправдати обраду података, али не може оправдати било какву обраду података**¹¹⁸. Управо се у овој разлици налази суштина баланса. Ако је, на пример, неопходно да здравствене власти обрађују одређене податке ради заштите јавног здравља, то не значи да су сви подаци о сваком грађанину аутоматски доступни свим институцијама. Ако је за спречавање одређеног облика криминала неопходно прикупити одређене податке, то не значи да се они могу чувати неограничено, користити за било коју другу сврху или учинити доступним сваком органу који за њих покаже интересовање. Сврха обраде мора остати јасна, а обим података ограничен на оно што је за њено остваривање неопходно.

У том смислу, равнотежа између јавног интереса и права личности служи пре свега једној ствари: **да ни јавни интерес не остане без заштите, али ни појединац не остане без правне границе која штити његову приватност и достојанство**. Правни поредак мора омогућити држави да делује онда када је њено деловање неопходно, али истовремено мора спречити да се позивање на јавни интерес претвори у средство за неограничено прикупљање и коришћење информација о грађанима.

На крају, значај овог баланса можда се најједноставније може изразити једном реченицом: **држава сме да зна онолико колико јој право и стварна потреба дозвољавају, али не сме да зна више само зато што јој технологија то омогућава**. У томе се и огледа суштина савремене заштите података о личности — не у апсолутној забрани њихове обраде, већ у захтеву да свака обрада има оправдан разлог, јасно одређену сврху, одговарајуће границе и одговорност која је прати. Код посебних врста података тај захтев постаје још снажнији, јер што је податак ближи најинтимнијој сфери личности, то мора бити ужи простор у којем јавни интерес може оправдати његову употребу.

¹¹⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, чл. 5 ст. 1, чл. 6 ст. 1 тач. е и ст. 3.

VI КОМПАРАТИВНА АНАЛИЗА

Компаративна анализа у области заштите података о личности не представља само упоређивање различитих законских текстова. Њен прави смисао састоји се у испитивању начина на који различити правни системи препознају исте или сличне ризике, како их нормативно уређују и, што је посебно значајно, како своја правила примењују у стварним животним ситуацијама. Заштита података о личности је област у којој се границе између националних правних поредака постепено губе. Развој дигиталних технологија, прекогранични токови података, глобалне платформе, електронска здравствена документација, биометријски системи и вештачка интелигенција довели су до тога да се исти или веома слични проблеми појављују у различитим државама, иако се њихова правна решења могу разликовати.

Управо зато упоредно право у овој области има посебну вредност. Оно омогућава да се национално решење сагледа изван његових сопствених граница. Правило које унутар једног правног система делује потпуно логично може, када се упореди са другим системима, показати одређене предности, али и слабости. С друге стране, решење које је развијено у једној држави не може се аутоматски пренети у другу, јер његова делотворност зависи од ширег институционалног, уставног, процесног и друштвеног контекста. Због тога циљ компаративне анализе није да се једноставно утврди „ко има бољи закон“, већ да се испита зашто је одређено решење настало, који проблем покушава да реши, како функционише у пракси и под којим условима би сличан приступ могао бити прихватљив у домаћем правном поретку¹¹⁹.

Компаративна анализа која следи, стога, има двоструку функцију. Прва је сазнајна, да покаже како се проблем заштите посебних врста података решава у три различита правна окружења. Друга се везује за могућност примене, да се утврди који елементи тих решења могу бити корисни за даљи развој српског система, а који су условљени специфичностима правних поредака у којима су настали. Самим тим, компаративно право овде није циљ само по себи, већ средство за боље разумевање домаћег права.

¹¹⁹ Konrad Zweigert, Hein Kötz, *An Introduction to Comparative Law*, 3rd ed., translated by Tony Weir, Oxford University Press, Oxford, 1998., стр. 34-35.

6.1 Упоредноправни преглед – Немачка, Француска и Велика Британија

6.1.1 Немачка

Немачка заузима посебно место у историји европске заштите података о личности. Њен значај не произлази само из чињенице да је једна од држава у којима је заштита података нормативно веома развијена, већ и из чињенице да је управо немачка уставносудска пракса снажно допринела обликовању идеје да човек мора имати одређени степен контроле над информацијама које се о њему прикупљају и користе.

Полазна тачка за разумевање немачког приступа јесте одлука Савезног уставног суда од 15. децембра 1983. године, донета поводом Закона о попису становништва. У тој одлуци Суд је извео право на информациону самосталност из општег права личности, заснованог на члану 2. став 1. у вези са чланом 1. став 1. Основног закона. Суд је нагласио да појединац, у начелу, мора имати могућност да сам одлучује о откривању и употреби својих личних података. Истовремено, Суд није поставио информациону самосталност као апсолутно право. Ограничења овог права могућа су ако служе претежном јавном интересу, ако су заснована на уставно прихватљивом законском основу, ако тај основ испуњава захтеве правне јасности и ако се поштује начело сразмерности.

Посебно је значајно што је немачки Уставни суд још тада препознао проблем који је данас постао један од централних проблема дигиталног доба: **значај једног податка не може се процењивати изоловано од могућности његове употребе, обраде и повезивања са другим подацима.** Суд је указао да податак који сам по себи делује безначајно може добити потпуно нови значај када се обрађује аутоматизовано и повезује са другим информацијама. На тај начин немачка уставносудска пракса је, још пре савремене експанзије интернета и великих база података, препознала да технолошке могућности обраде не мењају само количину доступних информација, већ и њихов значај за правни положај појединца¹²⁰.

¹²⁰ Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a., BVerfGE 65, 1 (43–44, 45), „Volkszählungsurteil“;

Овај приступ је изузетно важан за посебне врсте података о личности. Ако се, на пример, податак о здрављу посматра сам за себе, његов значај је очигледан. Али ако се он повеже са подацима о кретању, радном односу, финансијама или социјалном статусу, може се створити много дубља слика о животу појединца. Управо зато немачка доктрина информационе самосталности не полази искључиво од питања да ли је одређени податак „осетљив“, већ и од питања шта се са њим може учинити.

Тај уставни приступ данас је допуњен немачким савезним Законом о заштити података (Bundesdatenschutzgesetz – BDSG), који функционише у оквиру GDPR-а и садржи национална правила у областима у којима GDPR оставља простор државама чланицама.

Овде се већ може уочити прва важна разлика у односу на Србију. Србија, као држава која није чланица Европске уније, нема GDPR као директно применљиву уредбу у свом правном систему. Она је, међутим, у великој мери преузела његову концепцију кроз Закон о заштити података о личности. Немачки модел, напротив, представља комбинацију непосредне примене GDPR-а и националне разраде тамо где европски оквир то допушта.

Посебно је занимљив немачки приступ обради података у здравственом сектору и радном односу. Савезни радни суд Немачке је 20. јуна 2024. године донео одлуку у предмету 8 AZR 253/20¹²¹, који се односио на обраду здравствених података запосленог од стране Медицинске службе која је истовремено била и његов послодавац. Суд је прихватио да таква обрада може бити законита на основу члана 9. став 2. тачка h GDPR-а када је неопходна ради процене радне способности запосленог и када су испуњени законом прописани услови и гаранције. У конкретном случају, Суд је закључио да национални правни оквир не захтева аутоматско упућивање предмета другом медицинском органу само због чињенице да је пацијент истовремено запослен код органа који врши медицинску процену. Уместо тога, заштита поверљивости обезбеђује се кроз посебне законске и организационе гаранције, укључујући професионалну и службену обавезу чувања тајне, као и одговарајуће мере заштите приступа подацима. Суд је, дакле, прихватио могућност да исти субјект обрађује веома осетљиве здравствене податке свог

¹²¹ Bundesarbeitsgericht, Urteil des Achten Senats vom 20. Juni 2024 – 8 AZR 253/20, ECLI:DE:BAG:2024:200624.U.8AZR253.20.0, нарочито т. 37–49, 57, 60 и 80-82.;

запосленог, али само када за то постоји конкретан правни основ, јасно одређена сврха и одговарајуће гаранције поверљивости и безбедности података.

Овај приступ је веома поучан за Србију. У домаћем праву такође постоји могућност обраде посебних врста података када су испуњени услови предвиђени Законом о заштити података о личности. Међутим, немачки пример показује да није довољно да закон формално дозволи обраду. Потребно је да се у конкретном поступку може показати зашто је обрада неопходна, који се подаци користе, ко им приступа, за коју сврху и које мере спречавају њихову даљу употребу.

Још један занимљив аспект немачког система јесте веома снажан положај службеника за заштиту података. BDSG, поред правила GDPR-а, за јавне органе предвиђа именовање службеника за заштиту података и захтева његово благовремено укључивање у питања која се односе на заштиту података. Службеник мора бити независан у извршавању својих задатака и не сме добијати упутства у погледу њиховог вршења¹²². За Србију је ово посебно значајно јер Закон о заштити података о личности такође познаје институт лица за заштиту података о личности. Стога се немачко решење у овом делу не би морало „преносити“ у домаће право као нови институт; оно би пре могло послужити као практични стандард за тумачење постојећег института. Другим речима, Србији није неопходно да створи потпуно нову правну конструкцију, већ да постојећим механизмима обезбеди стварну независност, стручност и укљученост службеника у процесе обраде података.

Немачки модел, међутим, није у целини непосредно преносив у Србију. Пре свега, Немачка је федерална држава, са федералним и покрајинским органима заштите података, док је Србија унитарно организована држава са јединственим националним надзорним органом – Повереником за информације од јавног значаја и заштиту података о личности. Такође, немачка правила су део правног поретка Европске уније, што ствара додатни ниво правне контроле, укључујући улогу Суда правде Европске уније и механизме европске сарадње.

¹²² Вид. Bundesdatenschutzgesetz (BDSG), §§ 5–7, нарочито § 5 ст. 1 и 3 и § 6 ст. 1 и 3.

6.1.2 Француска

Француски систем заштите података о личности представља један од најзначајнијих европских примера снажне институционалне заштите приватности. Његова особеност нарочито се огледа у улози Националне комисије за информатику и слободе (Commission nationale de l'informatique et des libertés – CNIL)¹²³, која има дугу традицију надзора над обрадом података и која у пракси веома активно користи своја контролна и санкциона овлашћења.

Француска је, као држава чланица Европске уније, непосредно везана GDPR-ом, али национални оквир разрађује и допуњује кроз Закон о информатицији, датотекама и слободама (Loi Informatique et Libertés)¹²⁴. Посебан значај имају области у којима је француски законодавац искористио могућности које GDPR оставља државама чланицама, нарочито у здравственом сектору и истраживањима.

За тему овог рада посебно је занимљива чињеница да француски систем показује како се заштита посебних података може остваривати не само кроз опште забране и изузетке, већ и кроз **специјализоване поступке контроле и претходне процене**.

То се веома јасно види у области здравствених података. CNIL је 5. септембра 2024. године санкционисао компанију CEGEDIM SANTÉ новчаном казном од 800.000 евра због, између осталог, незаконите обраде здравствених података¹²⁵. Компанија је развијала и продавала софтвер који користе лекари у приватним ординацијама и здравственим центрима. Контролом је утврђено да су путем једног од софтверских решења обрађивани здравствени подаци који нису били анонимни, већ псеудонимизовани, а који су потом прослеђивани корисницима ради израде студија и статистика у области здравства. Посебно је било значајно постојање јединственог идентификатора пацијента, који је омогућавао

¹²³ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment art. 8, 19 et 20; Commission nationale de l'informatique et des libertés (CNIL), « Les missions de la CNIL »;

¹²⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016; Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, нарочито чл. 1–3.;

¹²⁵ Commission nationale de l'informatique et des libertés (CNIL), Délibération de la formation restreinte n° SAN-2024-013 du 5 septembre 2024 concernant la société CEGEDIM SANTÉ.

повезивање података достављених у различитим периодима и реконструкцију његовог пута лечења, што је, према оцени CNIL-а, стварало ризик од поновне идентификације.

Овај случај је посебно значајан јер показује један од кључних проблема савремене дигиталне економије: подаци прикупљени у једном контексту могу добити нову економску и аналитичку вредност када се повежу, обраде или користе у друге сврхе. Чињеница да је податак доступан одређеном субјекту, међутим, сама по себи не значи да тај субјект има неограничено право да га даље чува, повезује и користи. У дигиталном систему различите радње обраде могу технички бити међусобно повезане, али са правног становишта свака од њих мора имати одговарајући правни основ и бити ограничена сврхом због које се подаци обрађују. Управо зато информациони систем мора бити конципиран тако да технички подржава правне границе обраде, а не да их својим дизајном фактички потиरे.

Ово је веома применљиво и у Србији. Закон о заштити података о личности садржи исте основне принципе законитости, ограничења сврхе, минимизације и безбедности. Проблем, дакле, није у томе што српско право не познаје принцип који је CNIL применио. Напротив, тај принцип већ постоји. Оно што се може преузети из француског искуства јесте **начин његовог практичног спровођења** – детаљна контрола информационог система, испитивање конкретног тока података и санкционисање не само очигледних злоупотреба, већ и архитектонских решења која омогућавају прекомерну обраду.

Још један значајан пример представља одлука CNIL-а од 26. маја 2026. године, којом је компанији IQVIA OPERATIONS FRANCE изречена новчана казна од пет милиона евра због повреда правила о обради здравствених података у оквиру великих здравствених складишта¹²⁶. Случај је посебно значајан јер показује да легитимна сврха обраде, попут научног истраживања или унапређења здравствене заштите, сама по себи није довољна да оправда обраду посебних врста података. Неопходно је истовремено проценити ризике по права и слободе лица и обезбедити одговарајуће гаранције за њихово смањење. На тај начин француска пракса потврђује значај ризично оријентисаног приступа, према којем се

¹²⁶ Commission nationale de l'informatique et des libertés (CNIL), Délibération de la formation restreinte n° SAN-2026-008 du 26 mai 2026 concernant la société IQVIA OPERATIONS FRANCE.

законитост обраде не посматра само кроз њену сврху, већ и кроз обим, осетљивост и начин обраде података, као и мере предузете ради заштите лица.

Управо је то једна од области у којој француски приступ може бити посебно користан за Србију. Домаћи правни оквир већ познаје процену утицаја на заштиту података о личности и предвиђа њен значај нарочито код обрада које носе висок ризик, укључујући обраду посебних врста података у великом обиму и систематско праћење јавно доступних површина у великој мери. Пракса Повереника већ показује да се приликом процене ризика морају разматрати специфични ризици који произлазе из употребе нових технологија и биометријских података, а не само општа формула „људског фактора“.

Према томе, француско решење би у Србији могло бити примењено пре свега у **оперативном и институционалном смислу**. Није потребно преузети француски систем као целину, нити стварати нови орган. Повереник већ има надзорна и корективна овлашћења. Оно што би могло бити додатно развијано јесте пракса специјализованих контрола у секторима са посебно високим ризиком – здравство, биометријска идентификација, велики регистри, системи вештачке интелигенције и масовна аналитика података.

Са друге стране, нека француска решења не би могла бити непосредно пренета у Србију. Пре свега, Француска је држава чланица ЕУ и њен надзорни систем функционише у оквиру европског механизма сарадње. Поред тога, одређене посебне процедуре у области здравствених података произлазе из специфичног француског законодавства. Србија би могла преузети њихову **функционалну идеју**, али би конкретна правила морала бити прилагођена домаћем систему здравствене заштите, надлежностима Повереника и домаћем законодавству.

6.1.3 Велика Британија

Правни систем Велике Британије представља посебно занимљив предмет компаративне анализе, јер је његов развој у области заштите података истовремено снажно повезан са европским правом и обележен процесом издвајања из правног оквира Европске уније. Данас се у Великој Британији основни режим заштите података заснива на UK

GDPR-у и Data Protection Act 2018, уз новије измене које су унете Законом о коришћењу и приступу подацима из 2025. године (Data (Use and Access) Act 2025). Према актуелним смерницама ICO-а, посебне категорије података и даље обухватају податке који откривају расно или етничко порекло, политичка мишљења, верска или филозофска уверења, синдикално чланство, генетске и биометријске податке у сврху јединствене идентификације, податке о здрављу и податке о сексуалном животу или сексуалној оријентацији.¹²⁷

Основна концепција је, дакле, веома блиска GDPR моделу. За обраду посебних категорија података није довољно постојање општег правног основа; неопходно је испунити и посебан услов из члана 9 UK GDPR-а. У одређеним случајевима додатни услови и гаранције произлазе из Schedule 1 Data Protection Act 2018¹²⁸, којим се разрађују поједини услови за обраду посебних категорија података из члана 9 UK GDPR-а. За бројне облике такве обраде захтева се и посебан „appropriate policy document“, којим се документују услови на основу којих се обрада врши, поступци за поштовање основних начела заштите података, као и правила о чувању и брисању података.

Овај модел је занимљив за Србију јер показује један начин да се општа правила о посебним категоријама података допуне **секторским гаранцијама**. Велика Британија, на пример, предвиђа низ посебних услова за обраду ради значајног јавног интереса, здравства, социјалне заштите, истраживања и других сврха. Код одређених основа за обраду закон захтева и додатне гаранције, што спречава да се широко формулисан појам јавног интереса претвори у неограничено овлашћење за обраду.

Посебно значајан пример из британске праксе представља предмет *R (Bridges) v Chief Constable of South Wales Police*, који се односио на употребу аутоматизованог препознавања лица (AFR Locate) од стране полиције Јужног Велса. Током око 50 употреба система скенирано је приближно 500.000 лица, при чему је већина припадала лицима која нису била предмет полицијског интересовања. Апелациони суд Енглеске и Велса је 2020.

¹²⁷ UK General Data Protection Regulation, чл. 9; Data Protection Act 2018; Data (Use and Access) Act 2025; Information Commissioner's Office, "Special category data".

¹²⁸ Data Protection Act 2018, Schedule 1, Part 1 и Part 2, нарочито пар. 1–4 и 5, и Part 4, пар. 39; Information Commissioner's Office, "Special category data";

године утврдио да је конкретна употреба технологије била противна захтеву законитости из члана 8 Европске конвенције, између осталог због недовољно одређеног правног оквира за њену примену, а утврђени су и недостаци у процени утицаја на заштиту података. Значај овог предмета огледа се у томе што показује да употреба напредних биометријских технологија од стране јавних органа мора бити заснована на јасним правним правилима, подвргнута процени ризика и сразмерности и праћена одговарајућим гаранцијама заштите права лица.¹²⁹

Одговор који се може извући из овог предмета значајан је управо зато што се ослања на принципе. Технологија мора бити употребљена у оквиру јасних правила, за конкретно одређену сврху и уз одговарајућу контролу. Овакво размишљање је веома блиско европском принципу сразмерности и истовремено показује да биометријска технологија не сме бити посматрана само као техничко средство за идентификацију, већ као средство које може дубоко утицати на право на приватност.

Други значајан британски пример односи се на компанију *Clearview AI Inc.*, која је развила систем за аутоматизовано прикупљање фотографија лица са јавно доступних интернет страница и њихово претварање у претраживу базу за препознавање лица. У мају 2022. године британски Information Commissioner's Office (ICO) изрекао је компанији новчану казну од 7,5 милиона фунти и наложио јој да престане са обрадом података становника Велике Британије и да избрише већ прикупљене податке. Компанија је против одлуке уложила жалбу, па је питање примене британског права на њено пословање разматрано и пред First-tier Tribunal-ом, а потом и пред Upper Tribunal-ом. У октобру 2025. године Upper Tribunal је, између осталог, закључио да обрада података коју је Clearview вршио може представљати праћење понашања лица у Великој Британији и да чињеница да су његови корисници били страни државни и полицијски органи не искључује примену британског режима заштите података. Предмет је затим враћен First-tier Tribunal-у ради даљег одлучивања о суштини жалбе.¹³⁰

¹²⁹ Court of Appeal (Civil Division), *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police*, [2020] EWCA Civ 1058, 11 August 2020, нарочито т. 16, 152-153 и 210.

¹³⁰ *ICO v Clearview AI Inc (Privacy International intervening)*, [2025] UKUT 319 (AAC), Upper Tribunal (Administrative Appeals Chamber), 6 October 2025, нарочито т. 1–8, 89–94 и 115–121.

Значај овог предмета за заштиту посебних врста података огледа се у томе што показује да чињеница да је фотографија лица јавно доступна на интернету сама по себи не значи да је њена даља обрада за биометријску идентификацију слободна од правних ограничења. Предмет зато илуструје да се заштита личних података у дигиталном окружењу не може свести само на питање да ли је лице добровољно објавило одређену информацију, већ мора обухватити и начин, сврху и последице њене даље аутоматизоване обраде.

Овде се појављује једна од најважнијих лекција за Србију. Јавна доступност податка није исто што и неограничена доступност за сваку даљу обраду. Чињеница да је фотографија постављена на интернет не значи да сваки субјект може да је преузме, биометријски анализира, повеже са другим базама и користи за креирање система идентификације. Домаћи правни систем, кроз принципе законитости, ограничења сврхе и посебне услове за обраду биометријских података, већ садржи основу за такав закључак.

Истовремено, Clearview случај показује један проблем који се у Србији не може решити само изменом домаћег закона: **прекограничну примену права**. Када се компанија налази ван Србије, а обрађује податке лица која се налазе у Србији, поставља се питање домета домаћих правила, надлежности Повереника, могућности извршења одлуке и међународне сарадње. Управо због тога је европски систем заштите података развио сложена правила о територијалном домету и међународној сарадњи.

У том делу британски пример је само делимично применљив на Србију. Србија не може једноставно преузети механизам који произлази из положаја Велике Британије у односу на ЕУ, јер је њен међународноправни и институционални положај другачији. Али може преузети суштинску идеју, а то је да право заштите података мора бити способно да реагује на обраду која се дешава изван физичких граница државе, ако производи последице за њене грађане.

Велика Британија је занимљива и због чињенице да је задржала систем посебних категорија података сличан GDPR-у, али га је допунила сопственим националним гаранцијама. Data Protection Act 2018 предвиђа додатне услове за различите основе обраде,

укључујући запошљавање, здравство, значајан јавни интерес, истраживања и статистику. Код значајног јавног интереса закон садржи читав низ конкретних ситуација у којима је обрада дозвољена, али под додатним условима и гаранцијама.

За Србију је овај приступ занимљив јер би се у појединим секторима могла размотрити потреба за јаснијим **секторским гаранцијама**. На пример, код здравствених, биометријских или генетских података општа правила могу бити допуњена детаљнијим секторским прописима који јасно одређују ко сме да обрађује податке, у које сврхе, колико дуго, под којим условима и уз које мере заштите.

6.1.4 Компаративно сагледавање три модела и могућности примене у Србији

Када се немачки, француски и британски приступ посматрају заједно, постаје видљиво да, упркос различитим правним традицијама, постоји заједничка основа. Ниједан од ових система не полази од апсолутне забране обраде посебних врста података. Напротив, сви прихватају да су такве обраде у одређеним околностима неопходне. Оно што се разликује јесте начин на који се постављају границе и како се обезбеђује да изузетак не постане правило.

За Србију је прва важна поука да постојећи нормативни оквир већ има значајан степен сличности са европским системима. Закон о заштити података о личности из 2018. године преузео је велики број концепата GDPR-а, укључујући посебне врсте података, ограничење сврхе, минимизацију, процену утицаја, службеника за заштиту података и одговорност руковооца. Због тога би било погрешно закључити да је главни проблем у Србији непостојање правне основе.

Истовремено, управо компаративни примери показују да **нормативна сличност није исто што и практична једнакост**. У том смислу, Србија би могла да преузме неколико функционалних решења. Прво, може се додатно развијати **уставносудска и судска пракса у области заштите података**. Србија већ има члан 42. Устава, који изричито гарантује заштиту података о личности, као и праксу Уставног суда која се

односи на ову област. У одлуци ГУз-41/2010 од 30. маја 2012. године¹³¹ Уставни суд је, полазећи од члана 42. Устава Републике Србије, нагласио да прикупљање, држање, обрада и коришћење података о личности морају бити уређени законом, чиме је потврђено да се правни основ за обраду не може проширивати подзаконским актима и да законска заснованост представља једну од основних гаранција заштите права на заштиту података о личности.

Друго, могуће је јачати **превентивну функцију Повереника**. Француско искуство показује да надзор не треба да се активира само када је штета већ настала. Посебно у областима у којима се обрађују здравствени, генетски и биометријски подаци, контроле, смернице и превентивне мере могу бити подједнако значајне као санкције. То је у складу и са домаћим системом процене утицаја и процене ризика.

Треће, могуће је даље развијати **секторске гаранције**. Британски и немачки модели показују да општи закон није увек довољан за све специфичне ситуације. Здравство, радни односи, полицијска обрада, научна истраживања и биометријски системи имају различите ризике. Зато посебни прописи могу детаљније одредити начин приступа, рокове чувања, услове преноса, обавезу евидентирања приступа и друге мере.

Четврто, потребно је наставити са развојем **техничких и организационих мера као дела правне заштите**. Немачки случај здравствених података показује да законитост није довољна ако не постоје адекватне мере ограничења приступа. Француски случајеви здравствених база показују да је важно контролисати читав ток података, а британски случајеви биометријског препознавања показују да техничка могућност идентификације не значи аутоматски и правну дозвољеност. У Србији се овај приступ може развијати кроз примену принципа „privacy by design“, процену утицаја, минимизацију, псеудонимизацију, контролу приступа и евидентирање активности.

Најзад, посебну пажњу треба посветити **биометријским технологијама**. Ту је упоредна анализа нарочито корисна јер показује да се проблем не може решавати само питањем да ли је технологија ефикасна. Потребно је испитати њену неопходност, тачност,

¹³¹ Уставни суд Републике Србије, Одлука ГУз-41/2010 од 30. маја 2012. године, „Службени гласник РС“, бр. 68/2012.

ризик од грешке, обим примене, период чувања података, круг лица која се обрађују и могућност остваривања права лица. Британски предмет Bridges показује управо такав приступ.

У том погледу, можда је најважнија заједничка лекција сва три система управо то да **заштита посебних података није један правни институт, већ читав механизам**. Закон мора поставити услове, надзорни орган мора обезбедити контролу, судови морају обезбедити правну заштиту, а руковооци морају бити способни да правне захтеве преведу у конкретне процедуре и технологије. Ако било која од ових карика недостаје, формална заштита може постојати, али њена стварна делотворност остаје ограничена.

Најзад, из компаративног прегледа Немачке, Француске и Велике Британије може се извући један заједнички закључак: **делотворна заштита посебних врста података почиње тамо где право престаје да буде само апстрактна забрана, а постаје конкретан систем контроле над животом податка**. Потребно је знати зашто је податак прикупљен, ко га користи, коме може бити доступан, са чим се може повезати, колико дуго може бити чуван и шта се дешава када сврха због које је прикупљен престане да постоји. Управо су то питања која се, у различитим облицима, појављују у пракси све три анализиране државе.

6.2 Практична искуства у примени GDPR

Практична примена Опште уредбе о заштити података показала је да се ефикасност система заштите личних података не може мерити само степеном нормативне уређености, већ пре свега способношћу да се прописана начела и обавезе доследно примене у конкретним ситуацијама. Од ступања GDPR-а на снагу, европска пракса постепено је изградила приступ према којем се законитост обраде не процењује формално, већ у односу на њену стварну сврху, неопходност, обим, ризике по права и слободе лица и постојање одговарајућих мера заштите. Ово је нарочито значајно код посебних категорија података, чија обрада захтева виши степен опреза и оправданости.

Искуство европских надзорних органа показује да се најзначајнији изазови заштите података јављају управо у областима у којима технолошке могућности обраде превазилазе традиционалне начине прикупљања и употребе података. Здравствени, генетски и

биометријски подаци све се чешће обрађују у великим информационим системима, уз примену алгоритама, профилисања и различитих облика аутоматизованог доношења одлука, што истовремено отвара питања законитости, транспарентности, процене ризика и заштите права лица на која се подаци односе¹³². У таквим ситуацијама није довољно утврдити постојање правног основа за обраду, већ је неопходно испитати да ли је конкретна обрада заиста неопходна за одређену сврху, да ли се обрађује само неопходан обим података, ко им може приступити и колико дуго се чувају.

Посебно значајну улогу у практичној примени GDPR-а имају национални надзорни органи и Европски одбор за заштиту података. Њихова пракса показује да се принципи као што су минимизација података, ограничење сврхе, одговорност руковооца и безбедност обраде не смеју свести на формално испуњавање документационих обавеза. Процена утицаја на заштиту података, евиденције о обради, одређивање службеника за заштиту података, процена ризика и техничке и организационе мере имају стварни превентивни значај само ако су интегрисани у процес доношења одлука, а не ако постоје искључиво као административна документација.

Практична искуства такође показују да посебан режим заштите не значи апсолутну забрану обраде осетљивих података. Напротив, европски систем полази од контролисане допуштености, при чему је неопходно испунити како опште услове законитости обраде, тако и један од посебних услова предвиђених за обраду посебних категорија података. У пракси то захтева посебно пажљиво образложење сврхе и неопходности обраде, као и примену додатних гаранција којима се смањује могућност злоупотребе.

Једно од најзначајнијих практичних искустава примене GDPR-а јесте, стога, померање тежишта са накнадне реакције на превентивно деловање. Руковалац подацима није дужан само да поступа законито, већ мора бити у стању да покаже да је законитост обраде унапред процењена и да су предузете мере сразмерне ризицима. Овај приступ је посебно важан у областима у којима обрада може имати далекосежне последице по

¹³² Радна група из члана 29, *Смернице о аутоматизованом индивидуалном доношењу одлука и профилисању у сврхе Уредбе 2016/679*, WP251rev.01, усвојене 6. фебруара 2018. године, које је Европски одбор за заштиту података накнадно одобрио.

појединца, као што су здравство, запошљавање, безбедност, финансијске услуге и употреба биометријских технологија.

За Републику Србију практична искуства примене GDPR-а имају посебну вредност. Иако се GDPR не примењује као домаћи пропис, његова решења су у значајној мери послужила као узор за Закон о заштити података о личности. Стога искуство држава чланица Европске уније може бити значајно не само приликом даљег нормативног усклађивања, већ и у развијању домаће праксе Повереника, судова, руковалаца и обрађивача. Посебно су корисна искуства која показују како се општи принципи претварају у конкретне процедуре, техничке мере, процене ризика и механизме контроле.

6.3 Могућност примене добрих пракси у Србији

Компаративна анализа правних система Немачке, Француске и Велике Британије показује да се савремена заштита података о личности не исцрпљује у постојању одговарајућих законских норми. Иако је нормативни оквир неопходна полазна основа, стварна делотворност заштите зависи и од начина на који се те норме тумаче, примењују и контролишу, од институционалних капацитета, степена свести руковалаца и обрађивача, као и од техничких и организационих мера које се примењују у свакодневном поступању са подацима. Ово нарочито долази до изражаја код посебних врста података о личности, код којих последице незаконите или неадекватно обезбеђене обраде могу бити далеко озбиљније по права и слободе појединца.

У том смислу, питање примене добрих пракси у Републици Србији не треба схватити као питање механичког преузимања решења из других правних система. Добра пракса није нужно правило које постоји у страном законодавству, нити се њена вредност мери тиме што је примењена у држави са развијенијим институционалним механизмима. Она пре представља **проверен начин поступања који омогућава да се одређени правни принцип спроведе на делотворнији, предвидљивији и сигурнији начин**. Управо зато је код упоредноправног преношења неопходно разликовати оно што представља специфичност одређеног правног система од онога што има општију применљивост.

Посматрано из тог угла, из искуства Немачке може се издвојити нарочито значајна идеја информационог самоопредељења и захтева да ограничење права на заштиту личних података буде засновано на јасном правном основу, оправданој сврси и сразмерности. Немачка уставносудска пракса показала је да заштита података није само питање техничке поверљивости информација, већ питање односа појединца према сопственој личности и могућности да задржи одређени степен контроле над информацијама које га се тичу. Управо овај приступ може бити од значаја и за Србију, нарочито у ситуацијама у којима државни органи или друга лица располажу великим количинама података које могу међусобно повезивати и анализирати.

За српски правни систем посебно је значајна могућност да се **принцип сразмерности доследније примењује не само након што дође до повреде права, него већ у тренутку планирања одређене обраде**. На тај начин питање не би било само да ли је одређена обрада формално дозвољена, већ и да ли је заиста неопходна, да ли се иста сврха може постићи мањим обимом података и да ли постоји мање инвазиван начин поступања.

Француско искуство, са друге стране, указује на значај активне улоге независног надзорног органа и развијене праксе контроле. Деловање CNIL-а показује да заштита података постаје делотворнија када надзор није ограничен само на реаговање након повреде, већ обухвата и превентивно деловање, стручна упутства, секторске препоруке, контроле и санкционисање незаконитих обрада.

За Србију је овде важна једна релативно једноставна, али суштинска поука: **надзор над заштитом података не сме бити схваћен искључиво као репресивна функција**. Дobar систем надзора треба да делује и пре настанка повреде. У том смислу, Повереник већ располаже инструментима који омогућавају такав приступ. Посебно место има процена утицаја обраде на заштиту података о личности, која је Законом о заштити података о личности предвиђена за обраде које могу проузроковати висок ризик по права и слободе физичких лица. Повереник наглашава да ова процена треба да омогући руковооцу да сагледа ризике пре започињања обраде и да, уколико је то потребно, обраду прилагоди или од ње одустане.

Искуство Велике Британије посебно указује на значај контроле употребе нових технологија, а нарочито биометријских система. Савремени системи препознавања лица, аутоматизованог профилисања и анализе великих количина података показују да се традиционални правни приступи морају прилагођавати технологијама које омогућавају обраду података у размерама које раније нису биле могуће. За Србију је значајно то што Закон о заштити података о личности већ садржи механизме који могу представљати основу за одговор на такве изазове. Због тога основни проблем није нужно недостатак сваког појединачног правног инструмента, већ питање његове доследне и стручне примене.

При томе, постоје и реална **ограничења** примене страних добрих пракси. Прво ограничење представљају **разлике у институционалној структури**. Немачки систем почива на федералној организацији и постојању надзорних органа на различитим нивоима, док Србија има јединствени национални надзорни орган. Француски модел такође има институционалне специфичности које произлазе из њихове правне традиције, а британски систем је, након изласка из Европске уније, развио сопствени регулаторни оквир који се не може једноставно изједначити са GDPR-ом.

Друго ограничење односи се на **материјалне и кадровске капацитете**. Добра пракса која функционише у систему са великим бројем специјализованих стручњака, развијеном дигиталном инфраструктуром и значајним ресурсима за надзор не може се без измена применити у систему који располаже другачијим капацитетима. Стога је за Србију рационалније постепено унапређивање постојећих механизма него покушај њиховог потпуног преобликовања по моделу друге државе.

Треће, постоји и **културолошко и организационо ограничење**. Законска обавеза сама по себи не ствара културу заштите података. Ако се процена утицаја, евиденције обраде, интерне процедуре или лице за заштиту података посматрају само као формалност, њихова стварна заштитна функција остаје ограничена. Насупрот томе, ако се ти механизми схвате као средства за идентификовање ризика и унапређење пословања, они могу постати један од најважнијих инструмената превентивне заштите.

На крају, добра пракса у заштити посебних података о личности може се свести на једну суштинску идеју: **боље је спречити прекомерну или незакониту обраду него накнадно отклањати њене последице**. Такав приступ мења саму логику заштите – од реактивне ка превентивној, од формалне ка суштинској и од изолованог правног правила ка целовитом систему заштите. Управо у томе се може видети највећи простор за даљи развој српског система. Законодавни оквир Републике Србије већ садржи значајан број инструмената који омогућавају такав развој; наредни корак зато није нужно у стварању потпуно нових механизма, већ у њиховом доследнијем, стручнијем и практично оријентисаном спровођењу.

ЗАКЉУЧАК

У средишту сваке расправе о заштити података о личности, ма колико она била правно-техничка, на крају остаје човек. Закон може да говори о руковооцу, обрађивачу, правном основу, сврси обраде, минимизацији, роковима чувања и мерама безбедности, али иза сваког од тих појмова налази се једна иста вредност – право човека да одређени делови његовог живота остану под његовом контролом. Управо се у посебним врстама података та чињеница најјасније показује. Они не представљају само податке који су „осетљивији“ од других; они често откривају оно што човека одређује, његово здравље, порекло, уверења, идентитет, биолошке особености и најинтимније аспекте његовог живота. Зато је њихова заштита, у крајњем, заштита простора у којем личност остаје слободна.

Истраживање је показало да је савремени институт заштите посебних врста података настао као одговор права на једну дубоку промену: човек више није једини који памти податке о себи. Памте их институције, информациони системи, дигиталне платформе и базе података; они се умножавају, повезују, анализирају и понекад користе у сврхе које су удаљене од првобитног разлога њиховог прикупљања. Због тога се право на приватност више не може разумети искључиво као право да се други не мешају у приватни живот. Оно све више постаје право на разумну меру знања других о појединцу, право на информатичку аутономију и право да се о сопственој личности не постане само објекат туђег прикупљања и обраде информација.

У том смислу, посебне врсте података представљају један од најзначајнијих показатеља зрелости система заштите података о личности. Њихов посебан правни режим показује да једнакост свих података пред правом не би нужно значила и правичност. Напротив, различит степен ризика захтева различит степен правне заштите. Управо је зато савремени европски оквир, а нарочито Општа уредба о заштити података, развио посебне услове за њихову обраду, настојећи да успостави равнотежу између легитимних потреба друштва, јавног интереса, технолошког развоја и права појединца.

У Републици Србији је доношењем Закона о заштити података о личности из 2018. године направљен значајан корак ка приближавању овим стандардима. Међутим, анализа нормативног оквира, праксе, институционалне заштите и упоредноправних искустава показала је да хармонизација није тренутак у којем се доношењем једног закона завршава процес, већ трајан задатак правног поретка. Постојање европски конципираног законодавства представља неопходан, али не и довољан услов. Његова стварна вредност зависи од тога да ли се правила примењују у свакодневном раду органа власти, здравствених установа, послодаваца, образовних и других институција, као и од тога да ли појединац заиста може да оствари своја права.

Управо се ту показује значај практичне и институционалне димензије заштите. Повереник, судови, лица за заштиту података о личности, руковођи и обрађивачи не представљају одвојене тачке једног система, већ његове међусобно повезане елементе. Слабост једног од њих неминовно утиче на делотворност целине. Због тога даљи развој српског система не би требало да буде усмерен само на доношење нових правила, већ и на њихову доследну примену, јачање стручних и институционалних капацитета, развој судске праксе и стварање културе заштите података у којој се приватност не доживљава као препрека деловању, већ као граница одговорног деловања.

Упоредноправна анализа је, са друге стране, показала да не постоји један јединствени пут ка ефикасној заштити. Немачко искуство наглашава значај информационог самоопредељења и уставноправне контроле, француско искуство значај активног надзорног органа и превентивног деловања, док британска пракса нарочито показује како се класични принципи заштите суочавају са изазовима биометрије и нових

технологија. Смисао упоредног права зато није у механичком преузимању туђих решења, већ у препознавању оних принципа који могу бити прилагођени домаћем правном и институционалном контексту.

На основу свега изложеног, почетна хипотеза рада може се потврдити у својој суштини: Република Србија је остварила значајан степен нормативног приближавања европским стандардима, али између нормативне усклађености и пуне практичне делотворности и даље постоји простор који захтева континуирано унапређивање. Посебан изазов представљаће будући развој технологије, у којем ће могућност прикупљања и анализе података расти брже него што ће традиционалне правне категорије моћи да одговоре на све нове облике ризика. Управо зато заштита података мора бити способна да се развија, а да при томе не изгуби своје основно исходиште – човека.

Јер, на крају, право на заштиту података о личности није право на невидљивост, нити захтев да човек буде изузет из света информација. То је право на меру. Право да постоји граница између онога што о човеку може бити познато и онога што мора остати његово. Право да информација о личности не постане сама личност, нити да човек буде сведен на збир података који га описују. У времену у којем технологија све прецизније може да види, памти и предвиђа, највећи изазов права можда није у томе да спречи знање, већ да обезбеди да моћ знања никада не постане моћ над човеком.

САЖЕТАК

Овај рад се бави посебним врстама података о личности, њиховим правним карактеристикама, значајем за заштиту приватности и механизмима њихове заштите у правном систему Републике Србије. У раду се најпре разматрају појам и значај права личности, приватности и заштите података о личности, а затим се посебно анализирају посебне врсте података, као што су подаци о здрављу, генетски и биометријски подаци, подаци о расном или етничком пореклу, политичким и верским уверењима, сексуалном животу и сексуалној оријентацији. Посебна пажња посвећена је нормативном оквиру Републике Србије, пре свега Уставу и Закону о заштити података о личности, као и европским стандардима садржаним у Општој уредби о заштити података и Европској конвенцији о људским правима. Рад обухвата и анализу праксе Европског суда за људска права, улоге Повереника за информације од јавног значаја и заштиту података о личности, као и упоредноправни приказ решења у Немачкој, Француској и Великој Британији. Посебно се испитују степен усклађености српског законодавства са европским стандардима, практични проблеми у примени постојећих прописа и потреба за јачањем институционалне и судске заштите. Анализа показује да је Република Србија постигла значајан степен нормативне усклађености са европским стандардима, али да даљи напредак захтева доследнију примену прописа, усклађивање секторских законодавастава, јачање институционалних капацитета и развој делотворне судске праксе, нарочито имајући у виду све веће ризике који произлазе из дигитализације, употребе биометријских и генетских технологија, профилисања и других облика савремене обраде података о личности.

Кључне речи: посебне врсте података о личности; заштита података о личности; право на приватност; информациона аутономија; европски стандарди; Република Србија.

SUMMARY

This paper examines special categories of personal data, their legal characteristics, their significance for the protection of privacy, and the mechanisms for their protection within the legal system of the Republic of Serbia. The paper first considers the concept and significance of personality rights, privacy, and personal data protection, followed by an analysis of special categories of data, including data concerning health, genetic and biometric data, data revealing racial or ethnic origin, political and religious beliefs, sexual life, and sexual orientation. Particular attention is devoted to the normative framework of the Republic of Serbia, primarily the Constitution and the Law on Personal Data Protection, as well as European standards established by the General Data Protection Regulation and the European Convention on Human Rights. The paper also examines the case law of the European Court of Human Rights, the role of the Commissioner for Information of Public Importance and Personal Data Protection, and a comparative overview of legal solutions in Germany, France, and the United Kingdom. Particular consideration is given to the degree of harmonization of Serbian legislation with European standards, practical challenges in the application of existing regulations, and the need to strengthen institutional and judicial protection. The analysis demonstrates that the Republic of Serbia has achieved a significant degree of normative alignment with European standards, but that further progress requires more consistent application of regulations, harmonization of sector-specific legislation, strengthening of institutional capacities, and the development of effective judicial practice, particularly in view of the increasing risks arising from digitalization, biometrics, genetic technologies, profiling, and other forms of modern data processing.

Keywords: special categories of personal data; personal data protection; right to privacy; informational autonomy; european standards; Republic of Serbia.

СПИСАК КОРИШЋЕНЕ ЛИТЕРАТУРЕ

I АКАДЕМСКА И СТРУЧНА ЛИТЕРАТУРА

- 1) Aksoy, Hüseyin Can, „The Right to Personality and Its Different Manifestations as the Core of Personal Data“, *Ankara Law Review*, Vol. 5, No. 2, 2008, стр. 235–249.
- 2) Андоновић, С., Заштита података у електронској јавној управи у Републици Србији – правни аспекти, докторска дисертација, Правни факултет Универзитета у Београду, Београд, 2019.
- 3) Андоновић, С., Прља, Д., *Основи права заштите података о личности*, Београд: Институт за упоредно право, 2020.
- 4) Bevanda, Marko, Čolaković, Maja, „Pravni okvir za zaštitu osobnih podataka (u vezi sa zdravljem) u pravu Europske unije“, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, vol. 37, br. 1, 2016, стр. 125–154.
- 5) Buitelaar, J. C., „Post-mortem privacy and informational self-determination“, *Ethics and Information Technology*, Vol. 19, 2017, стр. 129–142.
- 6) Dulčić, K., Bodigoga-Vukobrat, N., „Zaštita osobnih podataka pacijenata u europskom i hrvatskom pravu“, стр. 371–411.
- 7) Fuster, Gloria González, De Hert, Paul, „The Legal Construction of Privacy and Data Protection“, *Computer Law & Security Review*, vol. 29, no. 5, 2013, стр. 522–530.
- 8) Gillet, Jeanne, *Privacy and Online Surveillance: International Legal Challenges*, PhD thesis, School of Law, University of Glasgow, 2019.
- 9) Jaramaz-Reskušić, Ivana, „Iniuria in pre-classical Roman law: concept and protection“, *Zbornik Pravnog fakulteta u Zagrebu*, Vol. 61, No. 2, 2011, стр. 545–571.
- 10) Johnson, Eric E., „Disentangling the Right of Publicity“, *Northwestern University Law Review*, vol. 111, br. 4, 2017, стр. 891–962.
- 11) Mann, Monique, Matzner, Tobias, „Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination“, *Big Data & Society*, Vol. 6, No. 2, 2019, стр. 1–11.
- 12) Mautner, Thomas, „Natural Law and Natural Rights“, у: Peter R. Anstey (ed.), *The Oxford Handbook of British Philosophy in the Seventeenth Century*, Oxford University Press, 2013, стр. 472–500.
- 13) Müller, Sigrid, „Concepts and Dimensions of Human Dignity in the Christian Tradition“, *Interdisciplinary Journal for Religion and Transformation in Contemporary Society*, Vol. 6, No. 1, 2020, стр. 24–25.
- 14) Quinn, Paul, Malgieri, Gianclaudio, „The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework“, *German Law Journal*, vol. 22, no. 8, 2021, стр. 1583–1585.
- 15) Schmitt-Maaß, Christoph, „‘Lumen Supernaturale’ vs ‘Lumen Naturale’: Human Rights and Their Religious Implications in Natural Law in the Early Enlightenment (Pufendorf–Thomasius–Wolff)“, *German Life and Letters*, vol. 78, br. 1, 2025, стр. 16–17.
- 16) Seren, Yvon, „L'exemple américain dans les institutions issues de la Révolution française ; les déclarations américaines et la déclaration française des Droits de l'Homme et du Citoyen de 1789“, *Annales de Bretagne et des pays de l'Ouest*, t. 84, br. 3, 1977, стр. 283.
- 17) Симоновић, И., Лазих, М., „Грађанскоправна заштита права личности“, *Зборник радова Правног факултета у Нишу*, бр. 68, 2014, стр. 270–272, 281–283.
- 18) Talapina, Elvira, „The Right to Informational Self-Determination: On the Edge of Public and Private“, *Law. Journal of the Higher School of Economics*, vol. 15, no. 5, 2022, стр. 24–25.
- 19) Thouvenin, F., „Informational Self-Determination: A Convincing Rationale for Data Protection Law?“, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 12, No. 4, 2021, стр. 246–250.
- 20) Van der Waerdt, Paul, „Information asymmetries: recognizing the limits of the GDPR on the data-driven market“, *Computer Law & Security Review*, vol. 38, 2020, art. 105436.
- 21) Warren, Samuel D., Brandeis, Louis D., „The Right to Privacy“, *Harvard Law Review*, vol. 4, br. 5, 1890, стр. 193–195.
- 22) Zweigert, Konrad, Kötz, Hein, *An Introduction to Comparative Law*, 3rd ed., translated by Tony Weir, Oxford University Press, Oxford, 1998.
- 23) Марковић, Р., „Сретењски устав – The Serbian ‘Sretenje’ Constitution“, *Анали Правног факултета у Београду*, год. 33, бр. 2, 1985, стр. 149–160.

- 24) Марковић, Р., *Уставно право*, Правни факултет Универзитета у Београду – Досије студио, Београд, 2015.

II НОРМАТИВНИ И ДРУГИ ПРАВНИ ИЗВОРИ

Национални нормативни извори

- 1) Устав Републике Србије, „Службени гласник РС“, бр. 98/2006.
- 2) 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.
- 3) Закон о заштити података о личности, „Службени лист СРЈ“, бр. 24/98 и 26/98 – исправка.
- 4) Закон о заштити података о личности, „Службени гласник РС“, бр. 97/2008.
- 5) Закон о заштити података о личности, „Службени гласник РС“, бр. 87/2018.
- 6) Закон о слободном приступу информацијама од јавног значаја, „Службени гласник РС“, бр. 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021.
- 7) Стратегија заштите података о личности за период од 2023. до 2030. године, „Службени гласник РС“, бр. 72/2023.
- 8) Акциони план за период од 2025. до 2027. године за спровођење Стратегије заштите података о личности за период од 2023. до 2030. године, 2025.

Европски и међународни нормативни извори

- 1) Регулација (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године о заштити физичких лица у односу на обраду података о личности и о слободном кретању таквих података и о стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података – GDPR), OJ L 119, 4. 5. 2016, стр. 1–88.
- 2) Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012.
- 3) Европска конвенција за заштиту људских права и основних слобода, 1950.
- 4) Конвенција о заштити лица у односу на аутоматску обраду података о личности, ETS бр. 108, Стразбур, 28. јануар 1981.
- 5) Директива 95/46/ЕЗ Европског парламента и Савета од 24. октобра 1995. године о заштити физичких лица у односу на обраду података о личности и о слободном кретању таквих података, OJ L 281, 23. 11. 1995.
- 6) Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, restructuring the control machinery established thereby, ETS No. 155, Strasbourg, 11 May 1994.
- 7) Code civil des Français, 1804, art. 1382.
- 8) Bürgerliches Gesetzbuch (BGB), 1900, § 12.
- 9) Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (KUG), 1907, §§ 22–23.
- 10) Bundesdatenschutzgesetz (BDSG), §§ 5–7.
- 11) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- 12) UK General Data Protection Regulation (UK GDPR).
- 13) Data Protection Act 2018.
- 14) Data (Use and Access) Act 2025.

Судска и надзорна пракса

- 1) Уставни суд Републике Србије, Одлука IУз-41/2010 од 30. маја 2012. године, „Службени гласник РС“, бр. 68/2012.
- 2) Билтен Уставног суда 2012–2016, књ. I, Београд, 2018.
- 3) Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 u. a., BVerfGE 65, 1–88 („Volkszählungsurteil“).

- 4) Bundesarbeitsgericht, Urteil des Achten Senats vom 20. Juni 2024 – 8 AZR 253/20, ECLI:DE:BAG:2024:200624.U.8AZR253.20.0.
- 5) Court of Justice of the European Union, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18, Judgment of 16 July 2020.
- 6) Court of Justice of the European Union, ND and Others v. Digi Communications NV, C-77/21, Judgment of 20 October 2022.
- 7) ECtHR, Matijašević v. Serbia, no. 23037/04, Judgment of 19 September 2006.
- 8) European Court of Human Rights, Klass and Others v. Germany, no. 5029/71, judgment of 6 September 1978.
- 9) European Court of Human Rights, Leander v. Sweden, no. 9248/81, judgment of 26 March 1987.
- 10) European Court of Human Rights, Amann v. Switzerland [GC], no. 27798/95, judgment of 16 February 2000.
- 11) European Court of Human Rights, S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, judgment of 4 December 2008.
- 12) European Court of Human Rights, Roman Zakharov v. Russia [GC], no. 47143/06, judgment of 4 December 2015.
- 13) European Court of Human Rights, Catt v. the United Kingdom, no. 43514/15, judgment of 24 January 2019.
- 14) European Court of Human Rights, Benedik v. Slovenia, no. 62357/14, judgment of 24 April 2018.
- 15) European Court of Human Rights, Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13, 62322/14 and 24969/15, judgment of 25 May 2021.
- 16) Court of Appeal (Civil Division), R (on the application of Edward Bridges) v The Chief Constable of South Wales Police, [2020] EWCA Civ 1058, 11 August 2020.
- 17) ICO v Clearview AI Inc (Privacy International intervening), [2025] UKUT 319 (AAC), Upper Tribunal (Administrative Appeals Chamber), 6 October 2025.
- 18) Commission nationale de l'informatique et des libertés (CNIL), Délibération de la formation restreinte n° SAN-2024-013 du 5 septembre 2024 concernant la société CEGEDIM SANTÉ.
- 19) Commission nationale de l'informatique et des libertés (CNIL), Délibération de la formation restreinte n° SAN-2026-008 du 26 mai 2026 concernant la société IQVIA OPERATIONS FRANCE.
- 20) Commission nationale de l'informatique et des libertés (CNIL), Délibération de la formation restreinte n° SAN-2026-009 du 21 juillet 2026 concernant la société HÔPITAL PRIVÉ DE LA LOIRE.
- 21) Prezes Urzędu Ochrony Danych Osobowych, decyzja DKN.5131.57.2022, 13. jun 2024.

III ИЗВОРИ СА ИНТЕРНЕТА И СЛУЖБЕНИ ЕЛЕКТРОНСКИ ИЗВОРИ

- 1) European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, adopted 20 October 2020.
- 2) European Data Protection Board, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 2.0, 17 May 2023.
- 3) European Data Protection Board, *Guidelines 08/2020 on the targeting of social media users*, Version 2.0, 13 April 2021.
- 4) Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251rev.01, 6 February 2018.
- 5) European Data Protection Board, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*, WP248 rev.01, 4 October 2017.
- 6) European Data Protection Board, „Technology“, *AI and Technology*, доступно на: https://www.edpb.europa.eu/topics/ai-and-technology_en.
- 7) European Commission, „Application of the GDPR“, *Data Protection*, Reference to Regulation (EU) 2016/679.
- 8) European Commission, *Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25 January 2012.
- 9) European Commission, *A European strategy for data*, 2026.

- 10) European Data Protection Supervisor (EDPS), *Opinion 7/2015: Meeting the challenges of big data – A call for transparency, user control, data protection by design and accountability*, 19 November 2015.
- 11) European Data Protection Supervisor (EDPS), *Review of the EDPS mandate, 2015–2019*, одељак „Data protection goes digital“.
- 12) European Data Protection Supervisor (EDPS), „The Accountability Initiative“, 7 June 2016.
- 13) European Court of Human Rights, „The Situation before 1 November 1998“, у: *The European Court of Human Rights: Historical Background, Organisation and Procedure*.
- 14) Council of Europe, Treaty Office, *Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No. 5 – Full list of signatures and ratifications — Serbia*.
- 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 2019. годину*, Београд, 2020.
- 16) 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 2020. годину*, Београд, март 2021.
- 17) 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 2025. годину*, Београд, 2026.
- 18) Повереник за информације од јавног значаја и заштиту података о личности, *Извештај о спровођењу Закона о слободном приступу информацијама од јавног значаја и Закона о заштити података о личности у 2024. години*, Београд, 2025.
- 19) Повереник за информације од јавног значаја и заштиту података о личности, *Заштита података о личности: ставови, мишљења и пракса Повереника*, Београд, 2023.
- 20) Повереник за информације од јавног значаја и заштиту података о личности, „Руководице – заштита података о личности“, доступно на: <https://poverenik.rs/zastita-podataka/obaveze-rukovaoca/>.
- 21) Повереник за информације од јавног значаја и заштиту података о личности, „Како да остварите своја права?“, одељак „Зашто је важна заштита података о личности?“, доступно на: <https://poverenik.rs/zastita-podataka/kako-da-osvarite-svoja-prava/>.
- 22) Повереник за информације од јавног значаја и заштиту података о личности, „Корисни савети – Заштита података о личности“.
- 23) Повереник за информације од јавног значаја и заштиту података о личности, „Обуке“, ажурирано 13. јула 2026. године.
- 24) Повереник за информације од јавног значаја и заштиту података о личности, „Наставак обука из примене ЗЗПЈЛ за чланове Уније послодаваца Србије“, 12. мај 2026. године.
- 25) Повереник за информације од јавног значаја и заштиту података о личности, „Смернице, препоруке и најбоље праксе у вези са заштитом података о личности – Европски одбор за заштиту података“.
- 26) Повереник за информације од јавног значаја и заштиту података о личности, „Водич кроз судску праксу Европског суда за људска права у вези са заштитом података на српском језику“.
- 27) Повереник за информације од јавног значаја и заштиту података о личности, „Састанак Радне групе за измене и допуне Закона о заштити података о личности“, 10. април 2025. године.
- 28) Министарство правде Републике Србије, *Полазна основа за припрему Нацрта закона о заштити података о личности*, 2025.
- 29) NIST, *SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations*, Gaithersburg, 2020.
- 30) Scarfone, K. A., Souppaya, M. P., Cody, A., Orebaugh, A., NIST, *SP 800-115, Technical Guide to Information Security Testing and Assessment*, 2008.
- 31) ENISA, *Data Protection Engineering*, January 2022.
- 32) ENISA, *Risk Management Standards*, 2022.
- 33) ISO/IEC 27001:2013, A.10.
- 34) ISO/IEC 27033-1:2015, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*.
- 35) Commission nationale de l'informatique et des libertés (CNIL), „Les missions de la CNIL“.
- 36) European Data Protection Board, „Health data breach: the CNIL fined Hôpital Privé de la Loire 500 000 EUR“, 9 September 2026.
- 37) European Data Protection Board, „Polish SA: fine of 9 300 € for Independent Public Health Care Centre after hacker attack“, 28 November 2024.

БИОГРАФИЈА

Милица Пауновић рођена је 2001. године у Прокупљу. Основно образовање завршила је као ђак генерације, док је током средње школе остварила запажене успехе и исту је завршила са одличним успехом. Још током школовања показивала је изражену радозналост, истрајност и посвећеност учењу, особине које су касније постале важан део њеног академског развоја.

Основне академске студије на Правном факултету у Нишу завршила је септембра 2024. године, након чега наставља своје академско усавршавање на мастер студијама у области права, са посебним интересовањем за питања заштите људских права, права личности и заштите података о личности.

Поред права, Милица је велики љубитељ књижевности. Књигу доживљава не само као извор знања и уметничког искуства, већ и као простор у којем човек учи да разуме другог, али и себе. Управо спој правне мисли и књижевности представља једно од њених посебних интересовања, будући да у оба подручја препознаје заједничку тежњу ка разумевању човека, његових избора, слободе, одговорности и односа према другима.

Као чланица Адвокатске коморе Ниша, своје професионално усмерење види у адвокатури, којој жели да посвети будући професионални рад, настојећи да кроз знање, одговорност и посвећеност праву допринесе заштити права и интереса својих будућих клијената.

ИЗЈАВА О ИСТОВЕТНОСТИ
ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: Милица Пауновић

Наслов мастер рада „Посебни подаци о личности“

Ментор: Проф. др Милош Прица

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

У Нишу, _____

Потпис аутора

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом „Посебни подаци о личности“ пријављен и одбрањен на Правном факултету Универзитета у Нишу:

- резултат сопственог истраживачког рада;
- да овај мастер рад у целини, нити у деловима, нисам пријављивала на другим факултетима, нити универзитетима;
- да нисам повредила ауторска права, нити злоупотребила 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: Милица Пауновић

У Нишу, _____

Потпис аутора
