УНИВЕРЗИТЕТ У НИШУ

ПРАВНИ ФАКУЛТЕТ

Заштита података о личности у домену вештачке интелигенције

(мастер рад)

Ментор

Проф. др Милош Прица

Студент

Александра Миљковић

Број индекса М011/24-ИТ

Ниш, 2026. године

САДРЖАЈ

УВОД.....3

I ОДРЕЂИВАЊЕ ПОЈМА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ 6

1. Дефинисање вештачке интелигенције.....6

2. Подела вештачке интелигенције 9

II ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У ПРИМЕНИ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У ПРАВНОМ СИСТЕМУ ЕВРОПСКЕ УНИЈЕ.....11

1. Заштита података о личности у међународном правном оквиру 11

1.1. Заштита података о личности у докеумнетима Уједињених нација.....11

1.2. Заштита података о личности у документима Савета Европе.....12

1.3. Заштита података о личности у документима Европске уније 13

2. Општа уредба о заштити података и примена на системе вештачке интелигенције.....14

2.1. Акт о вештачкој интелигенцији – успостављање регулаторног оквира заснованог на ризику.....18

2.2. Системи високог ризика као фокусна тачка регулаторне контроле.....19

2.3. Упоредна анализа Опште уредбе о заштити података и Акта о ВИ.....21

III ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У ПРИМЕНИ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У РЕПУБЛИЦИ СРБИЈИ.....23

1. Развој заштите података о личности у домаћем праву.....23

2. Закон о заштити података о личности и примена вештачке интелигенције 26

2.1. Начела обраде података у примени вештачке интелигенције 26

2.2. Законитост обраде и примена вештачке интелигенције.....31

2.3. Обрада посебних врста података о личности и примена вештачке интелигенције 35

2.4. Право на ограничење обраде у примени вештачке интелигенције 37

2.5. Аутоматизовано доношење појединачних одлука и профилисање у примени вештачке интелигенције 38

2.6. Мере заштите у примени вештачке интелигенције 40

2.7. Безбедност обраде у примени вештачке интелигенције 41

2.8. Процена утицаја на заштиту података о личности у примени вештачке интелигенције 42

2.9. Претходно мишљење Повереника у примени вештачке интелигенције.....43

ЗАКЉУЧАК.....45
ЛИТЕРАТУРА 48
САЖЕТАК.....54
SUMMARY
……..…
……..56
БИОГРАФИЈА 58

УВОД

Еволуција људске цивилизације неминовно је везана за технолошке скокове, али четврта индустријска револуција, предвођена вештачком интелигенцијом, доноси изазове који превазилазе оквире техничког напретка и задиру у саму суштину правног поретка и људских права. Живимо у ери у којој податак више није само пасивна информација или статистички запис, већ примарни ресурс моћи, економске вредности и друштвеног утицаја. Вештачка интелигенција се конституисала као научна област паралелно са развојем рачунарства, али је њен савремени замах, заснован на машинском и дубоком учењу, трансформисао дигитални пејзаж из корена. Док су традиционални рачунарски системи функционисали на принципу детерминисаних низова упутстава, савремена вештачка интелигенција тежи репликацији људских когнитивних функција, развијајући способност аутономног закључивања и прилагођавања. Управо та трансформација која се огледа у преласку са крутог праћења инструкција на самостално учење из података представља фундаменталну тачку сукоба са правом на заштиту података о личности.

У средишту овог мастер рада лежи анализа дубоке и често парадоксалне тензије између технолошке експанзивности и правне рестриктивности. С једне стране, вештачка интелигенција инхерентно тежи ка „свезнању“; њена прецизност, било да је реч о медицинској дијагностици, аутономној вожњи или предиктивном маркетингу, директно зависи од количине и квалитета података којима се алгоритам тренира. С друге стране, правни оквир заштите приватности, грађен кроз деценије развоја међународних и домаћих норми, почива на принципима рестриктивности, ограничења сврхе и, пре свега, начелу минимизације података. Овај рад настоји да демистификује тај сукоб и одговори на питање

„како очувати информационо самоопредељење појединца у свету где алгоритми тзв. црне кутије могу реконструисати наш идентитет на основу наизглед небитних дигиталних трагова?“

Предмет овог истраживања је обухватна правна анализа механизама заштите података о личности у контексту примене система вештачке интелигенције. Анализа је постављена на три нормативна нивоа како би се добила потпуна слика регулаторног штита. Први ниво обухвата међународне документе Уједињених нација и Савета Европе, са посебним освртом на модернизовану Конвенцију 108. Други ниво фокусиран је на супранационални поредак Европске уније, где се анализира релација супсидијарности између Опште уредбе о заштити података и новог Акта о вештачкој интелигенцији. Трећи, и за нас најрелевантнији ниво, представља правни систем Републике Србије, где се истражује имплементација европских стандарда кроз домаћи Закон о заштити података о личности, Стратегију развоја вештачке интелигенције у Републици Србији за период 2025-2030.године и Етичке смернице за развој, примену и употребу поуздане и одговорне вештачке интелигенције.

Основни циљ рада је да кроз критичку анализу утврди да ли су постојећи правни инструменти довољни да зауздају специфичне ризике које генерише вештачка интелигенција, као што су алгоритамска пристрасност, нетранспарентност и масовни биометријски надзор. Рад тежи да докаже да заштита приватности у дигиталном добу више не може бити само „спољна“ правна обавеза, већ мора постати конститутивни елемент самог технолошког дизајна. Посебан циљ је анализа домаће праксе и улоге Повереника као институционалног гаранта који треба да спречи да економски интерес развоја алгоритама превлада над достојанством грађана.

У изради рада примењен је кумулативни приступ научних метода како би се материја сагледала из више углова. Правно-догматска метода коришћена је за прецизно тумачење законских одредаба и етичких принципа. Компаративна метода омогућила је уочавање јаза између теоријске заштите и реалне праксе технолошких гиганата, док су методе анализе и синтезе послужиле за повезивање техничких појмова, попут дубоког учења и неуронских мрежа, са њиховим правним последицама. Аксиолошка метода је проткана кроз цео рад, вреднујући свако технолошко решење кроз призму очувања људског достојанства.

Рад је структуриран тако да читаоца води од теоријских основа ка специфичним правним изазовима. Прво поглавље посвећено је дефинисању и подели вештачке интелигенције, од реактивних машина до концепта самосвесних система, чиме се поставља технички темељ за правну анализу. Друго поглавље детаљно разматра европски регулаторни оквир, анализирајући како Акт о вештачкој интелигенцији операционализује начела транспарентности и одговорности из Опште уредбе о заштити података. Треће поглавље представља аналитичко језгро рада, где се кроз призму домаћег Закона о заштити података о личности и Етичких смерница за тазвој, примену и употребу поуздане и одговорне вештачке интелигенције истражују начела обраде, законитост, обрада посебних категорија података, право на ограничење обраде, те кључни институти попут аутоматизованог одлучивања и процене утицаја на заштиту података.

На крају, овај увод служи као портал у материју у којој се преплићу математичка логика алгоритама и вредносни систем људских права. У свету где тзв. црна кутија вештачке интелигенције доноси одлуке о кредитној способности, запошљавању или медицинском лечењу, право не сме бити пасивни посматрач. Овај рад настоји да докаже да је право, упркос брзини технолошких промена, и даље једини ефикасан инструмент за очување суверенитета појединца над сопственим подацима и сопственим животом. Овај рад тежи ка дефинисању граница до којих технологија сме да иде, подсећајући нас да вештачка интелигенција мора остати алат у служби човека, а не аутономан ентитет који доноси неопозиве одлуке о људским судбинама.

I ОДРЕЂИВАЊЕ ПОЈМА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ

Како бисмо могли да доведемо у везу заштиту података о личности и употребу вештачке интелигенције неопходно је да се упознамо са појмом вештачке интелигенције. С тим у вези у овм делу рада пажњу ћемо посветити дефинисању вештачке интелигенције као и њеној подели.

1. Дефинисање вештачке интелигенције

Вештачка интелигенција (у даљем тексу: ВИ) се конституисала као научна област паралелно са развојем рачунарства, фокусирајући се на репликовање интелигентних функција попут дедукције и решавања проблема. Иако је терминолошки тешко прецизно одредити, један од првих концепата ВИ дефинише као кохезију науке и инжењерства у сврху креирања интелигентних машина и програма.[1] Често се ВИ дефинише и као област у оквиру које се истражује како да рачунари преузму оне послове у којима је људска интелигенција још увек надмоћна.[2] Такође, приликом дефинисања појма ВИ неки аутори заступају мишљење да је дефинисање ВИ у корелацији са методом којом се приступа ВИ.[3] Њопштије ВИ се може дефинисати као способност компјутера да опонашају људско размишљање и поступке.[4]

Давне 1950. конципирана је „игра имитације" (тзв. Тјурингов тест) као метод за евалуацију машинске интелигенције путем способности рачунара да симулира људску конверзацију.[5] Тест се сматрао успешним будући да је заварао проценат испитивача који је

[1] J. McCarthy, M. Minsky, N. Rochester, C. Shannon, A Proposal for the Dartmouth Summer Research Project on Artifiical Intelligence, *AI Magazine*, no. 27, vol. 4, 2006, 12-14.
[2] E. Wolfgang, *Grundkurs Künstliche Intelligenz: eine praxisorientierte Einführung*, Institut für Künstliche Intelligenz, Weingarten, 2016, 1.
[3] M. Scherer, Artificial Intelligence and Legal Decision-Making: The Wide Open?, *Journal of International Arbitration*, vol. 36, no. 5, 2019, 542.
[4] Merriam-Webster Dictionary, преузето 10.12.2025, https://www.merriam-webster.com/dictionary/artificial%20intelligence
[5] A. Turing, A Computing machinery and intelligence, *Mind*, vol.59, no. 236, 1950, 433-460.

могао оправдати његову успешност.[6] Иако су савремени рачунари еволуирали као физичке манифестације Тјурингових машина, они су и даље суштински ограничени на извршавање алгоритама, односно детерминисаних низова упутстава. Ово указује на фундаментални изазов који се огледа у немогућности решавања одређених математичких проблема пуним праћењем инструкција, што представља главну препреку у достизању вештачке опште интелигенције. Сви савремени софтвери и платформе суштински се заснивају на брзом извршавању огромног броја детерминисаних инструкција, при чему просечан рачунар у секунди обави операције за које би човеку биле потребне хиљаде година. Ипак, рачунари сами по себи не доносе одлуке, већ следе унапред дефинисане алгоритме. Кључни изазов ВИ је управо креирање система који, кроз прецизна упутства за учење, могу аутономно прилагођавати своје понашање.[7] Иако се одређени проблеми лако формализују у код, комплексност појединих области и даље представља значајну баријеру за потпуну примену интелигентних система.

Савремене дефиниције се класификују у четири категорије према два критеријума: фокусу на мисаоне процесе насупрот понашању, те оријентацији ка успеху извршења задатка.[8] Приликом дефинисања ВИ, научници се често ослањају на елементе поређења и приближности са људским когнитивним способностима.[9] Нарочита одлика људског разума, поред капацитета за стицање знања, јесте и модификовање сопствених поступака у складу са спољашњим околностима. Управо та вештина јасно разграничава људски интелект од машинске интелигенције као сегмента унутар ВИ. Способност независног доношења одлука се истиче као кључно обележје ВИ те се тако језгро ВИ огледа у томе да без туђе помоћи анализира огромне базе информација, да из њих самостално идентификује правилности, те да независно изводи закључке или процене. Овакви захтеви се, захваљујући механизмима ВИ, неретко извршавају ефикасније, а зависно од структуре самог система, такође и уз мање трошкова.[10]

---

[6] Д. Прља, Г. Гасми, В. Корач, *Вештачка интелигенција у правном систему ЕУ*, Институт за упоредно право, Београд, 2021, 63.
[7] M. Wooldridge, *A Brief History of Artificial Intelligence: What It Is, Where We Are, Where We Are Going*, Flatiron Books, Great Britain, 2021, 205.
[8] M. Furmankiewicz, A. Sołtysik-Piorunkiewicz, P. Ziuziański, *Artificial Intelligence and Multi-Agent Software for E-Health Knowledge Management System*, Informatyka Ekonomiczna, vol. 32, no. 2, 2014, 53.
[9] E. Wolfgang, *op. cit*., 2.
[10] Ibid.

Савремен приступ ВИ описује као симулацију људских когнитивних процеса путем алгоритама, фокусирајући се на креирање формалних модела понашања попут препознавања говора, креативности и медицинске дијагностике. Кључне функције ове области обухватају учење, планирање и решавање проблема, док се њена практична реализација ослања на међусобно повезане дисциплине попут науке о подацима, машинског и дубоког учења.[11] Продукт ВИ дефинише се као синтетизовани податак настао кроз процесе симулације људског резоновања приликом решавања постављених проблема. Овај процес се ослања на хијерархију дисциплина, почев од науке о подацима, која представља најшири оквир за откривање релевантних информација и њихових међусобних корелација. Унутар овог оквира, рударење података користи статистичке анализе и препознавање образаца како би се из великих скупова екстраховала употребљива знања, чиме се формира база за даље нивое интелигенције. Машинско учење омогућава системима да на основу историјских података самостално обрађују нове уносе без експлицитног програмирања инструкција. Суптилнији ниво представља дубоко учење, које путем сложених неуронских мрежа самостално идентификује кључне карактеристике унутар неструктурираних података. Коначно, појачано учење заснива се на систему награда и казни унутар затвореног окружења, где модел кроз итеративне покушаје самостално проналази оптимално решење проблема.[12] Основа ВИ почива на специјализованој хардверској инфраструктури и алгоритмима примарно кодованим у програмским језицима. Системи функционишу кроз детекцију образаца унутар обимних скупова података за обуку, што им омогућава предикцију будућих стања. Програмирање се суштински фокусира на три когнитивна аспекта: учење кроз прикупљање података и формирање алгоритама, закључивање путем одабира оптималних метода за постизање циља, те самоисправљање којим се континуирано ревидирају процеси ради веће прецизности. На тај начин, систем не само да извршава задатке, већ и непрестано усавршава сопствену ефикасност у обради информација.[13]

[11] H. Sroka, W. Wolny, *Inteligentne systemy wspomagania decyzji*, Wydawnictwo AE, Katowice, 2009, 167-172.
[12] Д. Прља, Г. Гасми, В. Корађ, *op. cit*., 65-67.
[13] *Ibid*., 67.

2. Подела вештачке интелигенције

Системи који теже симулацији људског когнитивног процеса и они базирани на рационалном закључивању примарно су фокусирани на процесе резоновања. Насупрот њима, категорије које обухватају системе са рационалним деловањем и системе који имитирају људске поступке акценат стављају на екстерно понашање. Успешност се мери двојако тачније кроз степен подударности са људским перформансама или кроз компарацију са идеалним концептом рационалности. Систем се дефинише као рационалан уколико адекватно поступа у складу са доступним информацијама. То подразумева пуну свест о циљу, односно постојање јасно дефинисане критеријумске функције која мери ефикасност деловања система у датом окружењу.[14] Иако је ова подела настала пре периода стагнације ВИ деведесетих година, она је задржала своју бухватност. Ипак, савремена достигнућа условила су нове систематизације према којима се дефинишу четири типа ВИ, чији дијапазон обухвата савремене апликативне задатке, па све до још увек нереализованих сензибилних система:

- Реактивне машине које представљају специјализоване системе без могућности депоновања меморије, који одлуке доносе искључиво на основу тренутне перцепције окружења. Примери попут програма Deep Blue и AlphaGo демонстрирају њихову способност за оптимално решавање конкретних задатака кроз анализу тренутног стања, без ослањања на претходна искуства,
- Системи са ограниченом меморијом који поседују способност депоновања података, што им омогућава да на основу претходних искустава доносе релевантне одлуке у будућности. Типичан пример система са ограниченом меморијом била би аутономна возила која континуирано прате променљиве параметре окружења, попут брзине других учесника у саобраћају, ради безбедног управљања и навигације,
- Теорија ума представља концепт будућих система са социјалном интелигенцијом који ће кроз разумевање људских емоција и намера омогућити директну сарадњу између машина и људи,

[14] М. Милосављевић. *Вештачка интелигенција*, Универзитет Сингидунум, Београд, 2015, 70.

- Самосовесне машине представљају финалну етапу развоја која подразумева креирање система са сопственом свешћу и капацитетом за разумевање личног унутрашњег стања. Овај концепт, који се изједначава са вештачком општом интелигенцијом, захтева потпуно дешифровање људског когнитивног апарата, укључујући меморију и доношење одлука на основу искуства.[15]

Алтернативна класификација у научној литератури разликује слабу и јаку ВИ, при чему се слаба дефинише као алат за специфичне задатке, док се јака поистовећује са самим когнитивним капацитетом мозга.[16] Док се слаба интелигенција примењује у оквиру уско дефинисаних операција попут виртуелних асистената, јака или општа ВИ тежи репликацији људске спознаје и аутономном решавању непознатих проблема уз примену фази (енг. *fuzzy*) логике.

На основу свега претходно наведеног можемо закључити да ВИ представља сложену и динамичну научну дисциплину чији је примарни циљ репликација људских когнитивних функција путем напредних рачунарских система и алгоритама. Иако у теорији не постоји јединствена дефиниција, она се суштински заснива на преласку са ригидног праћења инструкција ка аутономном учењу, закључивању и самоисправљању. Кроз еволуцију од реактивних машина до концепта самосвесних система, ова област тежи ка креирању модела који не само да обрађују податке енормном брзином, већ показују висок степен рационалности и прилагодљивости у решавању комплексних проблема.

[15] В. Спасић, Утицај вештачке интелигенције на ауторско право, у: Раичевић Н. (ур.), *Одговорност у правном и друштвеном контексту*, Тематски Зборник радова Правног факултета у Нишу, Ниш, 2023, 109.
[16] J. Searle, Minds, Brains, and Programs, *Behavioral and Brain Sciences*, vol. 3, no. 3, 1980, 417 – 424.

II ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У ПРИМЕНИ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У ПРАВНОМ СИСТЕМУ ЕВРОПСКЕ УНИЈЕ

Полазећи од предмета овог рада тј. заштите података о личности у примени ВИ сматрамо да би било од значаја да овом делу укажемо на међународни правни оквир којим се реглише заштита података о личности кроз документа Уједињених нација, Савета Европе и прву регултаиву у Европској унији. Након тога посебну пажњу усмерићемо на позитивно законодавство Европске уније како у вези са заштитом података о личности тако и у вези са регулисањем ВИ, како би смо у концу овог дела рада довели у везу заштиту података о личности у примени ВИ у Европској унији.

1. Заштита података о личности у међународном правном оквиру

Пре него што се упустимо у анализу кључних докумената који се односе на заштиту података о личности у Европској унији направићемо један кратак осврт на основне документе из којих је проистекао правни оквир карактеристичан за реалан временски интервал. С тим у вези у овом сегменту рада указаћемо на нека општа документа Уједињених нација, Савета Европе и Европске уније а који се оносе на заштиту података о личности.

1.1. Заштита података о личности у докеумнетима Уједињених нација

. У оквиру правног система Уједињених нација, акценат примарне заштите није стављен на податке о личности као засебну правну категорију, већ се они штите кроз шири институт права на приватност. Темељи ове заштите постављени су доношењем Опште декларације о људским правима[17], чиме је први пут на глобалном нивоу конституисана обавеза поштовања интиме појединца и спречавања арбитрарног уплитања, нарочито од стране државних

[17] Universal Declaration of Human Rights, 1948, art. 12, преузето 29.12.2025, https://www.un.org/en/about-us/universal-declaration-of-human-rights .

органа. Овај концепт је додатно оснажен кроз Међународни пакт о грађанским и политичким правима који изричито нормира неповредивост приватног и породичног живота, као и тајност кореспонденције. [18] Ипак, услед убрзане технолошке еволуције и дигитализације друштва, јавила се потреба за специфичнијом регулативом. Као одговор на ове изазове, Генерална скупштина Уједињених нација усвојила је резолуције о праву на приватност у дигиталној ери чиме је овај традиционални правни институт прилагођен савременим комуникационим околностима.[19]

1.2. Заштита података о личности у документима Савета Европе

У оквиру регионалног система Савета Европе, кључни инструмент заштите представља Европска конвенција за заштиту људских права и основних слобода[20]. Наведени правни механизам сваком појединцу обезбеђује право на поштовање приватног и породичног живота, као и заштиту интегритета дома и поверљивости комуникације. Иако се у самом тексту Конвенције не наводи експлицитно право на заштиту података о личности, оно је индиректно обухваћено кроз широку интерпретацију члана 8. Такав приступ је додатно потврђен и уобличен кроз богату и конзистентну јуриспруденцију Европског суда за људска права, који је заштиту информационе приватности подвео под окриље овог члана.[21]

У систему Савета Европе, знималајну улогу свакако заузима Конвенција о заштити лица у односу на аутоматску обраду личних података која је усвојена 1981. године и накнадно

---

[18] Закон о ратификацији међународног пакта о грађанским и политичким правима, *Службени лист СФРЈ*, бр. 7/71, чл. 17.

[19] Прва резолуција о праву на приватност донета је 2013. године Resolution adopted by the General Assembly on 18 December 2013, 68/167. The right to privacy in the digital age, преузето 4.2.2026 https://documents.un.org/doc/undoc/gen/n13/449/47/pdf/n1344947.pdf, док је друга резолуција усвојена 2016. године Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/, преузето 4.2.2026. https://digitallibrary.un.org/record/848969?ln=en&v=pdf .

[20] Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода, измењене у складу са Протоколом број 11, Протокола уз Конвенцију за заштиту људских права и основних слобода, Протокола број 4 уз Конвенцију за заштиту људских права и основних слобода којим се обезбеђују извесна права и слободе које нису укључене у Конвенцију и Први протокол уз њу, Протокола број 6 уз Конвенцију за заштиту људских права и основних слобода о укидању смртне казне, Протокола број 7 уз Конвенцију за заштиту људских права и основних слобода, Протокола број 12 уз Конвенцију за заштиту људских права и основних слобода и Протокола број 13 уз Конвенцију за заштиту људских права и основних слобода о укидању смртне казне у свим околностима, Службени лист СЦГ – Међународни уговори, бр. 9/2003, 5/2005, 7/2007 – испр., и Службени гласник РС – Међународни уговори, бр. 12/2010 и 10/2015.

[21] С тим у вези на овом месту указаћемо на једну од бројних представки *Case of Malone v. the United Kingdom*, Application no. 8691/79, 2 August 1984, преузето 3.2.2026, https://hudoc.echr.coe.int/eng?i=001-57533 .

ревидирана Модернизационим протоколом из 2018. године[22]. Овај инструмент представља јединствен, правно обавезујући међународни уговор специјализован за домен информационе приватности. Његово поље примене обухвата све облике обраде података, без обзира на то да ли се спроводе унутар јавног или приватног сектора. Сходно томе, ратификација овог акта намеће свим правним субјектима у државама уговорницама стриктну обавезу поштовања прописаних стандарда ради ефикасне заштите личних података.

1.3. Заштита података о личности у документима Европске уније

У правном поретку Европске уније, заштита података о личности конституисана је као аутономно право кроз члан 8. Повеље о основним правима Европске уније, који појединцима изричито јемчи овлашћење на приступ прикупљеним информацијама, као и захтев за њихову корекцију.[23] Регулаторни оквир је првобитно обликован Директивом 95/46/ЕЗ[24], која је поставила фундаменталне принципе и рестрикције у овој сфери. Ипак, суочена са изазовима дигиталне трансформације, Унија је извршила темељну реформу законодавства усвајањем Опште уредбе о заштити података 2016. године. Овај системски акт, чија је примена отпочела 25. маја 2018. године, увео је стриктније стандарде и модернизовао механизме заштите у складу са савременим технолошким развојем.

[22] Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), преузето 5.2.2026, https://rm.coe.int/16808ac918 .
[23] Charter of Fundamental Rights of the European Union (2000/C 364/01), art. 8, преузето 5.2.2026 https://www.europarl.europa.eu/charter/pdf/text_en.pdf
[24] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, преузето 5.2.2026 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 .

2. Општа уредба о заштити података и примена на системе вештачке интелигенције

У савременом правном поретку Европске уније, Општа уредба о заштити података (у даљем тексту: ГДПР)[25] представља примарни и технолошки неутралан инструмент који регулише сваку обраду података о личности, без обзира на техничка средства која се користе. Међутим, примена ових норми на системе ВИ отвара низ комплексних правних питања, с обзиром на то да су фундаментални принципи заштите приватности конципирани у ери статичне обраде података, док је ВИ заснована на динамичком учењу, предикцији и аутономности.

Највеће доктринарно спорење јавља се у покушају усклађивања начела минимизације са природом машинског учења. Начело минимизације података, утврђено чланом 5, ст. 1, тачка ц ГДПР, прописује да подаци морају бити „ограничени на оно што је неопходно у односу на сврху" за коју се обрађују. Анализа овог стандарда води нас ка томе да појам неопходности не сме бити тумачен кроз субјективну жељу програмера за већом прецизношћу модела, већ кроз објективну оправданост прикупљања сваког појединачног податка. Према мишљењу неких аутора овај императив захтева строгу селективност већ у фази дизајна система, чиме се онемогућава пракса прикупљања огромних сетова података под изговором потенцијалне будуће корисности.[26] У пракси, то значи да ако систем ВИ за аутоматизовану регрутацију кадрова може да донесе поуздану процену на основу образовања и радног искуства, прикупљање података о хобијима или присуству на друштвеним мрежама постаје незаконито, јер излази из оквира онога што је неопходно у односу на сврху професионалне селекције. Наведено даље генерише фундаменталну тензију између онога што се дефинише као сукоб између правне рестриктивности и технолошке експанзивности.[27] Правна

[25] 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), преузето 3.12.2025, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[26] A. L. Bygrave, *Information Law: From the Incunabula of Privacy to the Eras of Big Data and Artificial Intelligence*, Oxford University Press, Oxford, 2014, 142–145.

[27] M. Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Cheltenham, 2015, 78.

рестриктивност служи као заштитни механизам који поставља границе обради како би се очувао интегритет појединца, док технолошка експанзивност представља унутрашњи сегмент алгоритама ка континуираном учењу из што већег броја корелација.[28] Док технологија тежи ка свеобухватном знању, право инсистира на рестриктивном приступу подацима. Неки аутори заступају мишљење да би попуштање пред технолошком експанзивношћу могло довести до ерозије права на приватност, јер алгоритми често откривају сензитивне информације о појединцу из наизглед небитних података.[29] Стога, правна рестриктивност овде делује као нужан корективни фактор који нужно захтева од инжењера да техничка решења креирају унутар закона, а не изван њега. Једно од таквих решења које се афирмисало у теорији и пракси ЕУ јесте концепт под називом „минимизација приступа". За разлику од традиционалног концепта који тежи физичком смањењу броја података, минимизација приступа се фокусира на структуру система која омогућава учење на подацима без њиховог стварног разоткривања контролору (руковаоцу) или трећим странама.[30] Овај приступ је кључан јер омогућава да се задовољи технолошка потреба за подацима, а да се истовремено испоштује право на приватност. Примера ради овде бисмо могли навести здравствени сиситем који омогућава систему ВИ да анализира медицинске снимке на локалним серверима болница, док се ка централном алгоритму шаљу само апстрактни статистички модели. На тај начин се врши минимизација приступа личним медицинским подацима пацијената, чиме се ризик од злоупотребе или неовлашћеног откривања идентитата своди на минимум, а сврха унапређења дијагностике остаје остварена. Друго кључно начело је ограничење сврхе (чл. 5, ст. 1, тачка б), које представља један од најзахтевнијих регулаторних бедема за системе ВИ. Под термином „ограничење сврхе" подразумева се правна обавеза да подаци буду прикупљени у конкретне, јасно дефинисане и легитимне сврхе, те да се касније не смеју обрађивати на начин који није у складу са првобитним намерама. Системи ВИ често откривају нове корелације међу подацима које нису биле предвидиве у тренутку прикупљања, што ствара ризик од тзв.

[28] *Ibid*.
[29] L. Floridi, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities,* Oxford University Press, Oxford, 2019, 210.
[30] European Data Protection Board (EDPB), *Guidelines 04/2019 on Article 25 Data Protection by Design and by Default*, 12, преузето 10.11.2025. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

ширења функција. Израз „ширење функција“ означава постепену експанзију употребе система или скупа података изван граница за које је првобитно пројектован, често без знања или пристанка лица на које се подаци односе.[31] Према мишљењу појединих аутора овај принцип служи као заштита од неконтролисане моћи алгоритама да трансформишу обичне податке у алате за дубински надзор појединца.[32] У ситуацијама када алгоритам користи податке прикупљене за једну намену како би вршио профилисање кредитног ризика, поставља се фундаментално питање законитости такве секундарне обраде. Према једном мишљењу нужно је за сваку накнадну обраду утврдити постојање спојивости са првобитном сврхом.[33] С тим у вези се наглашава да се спојивост не сме претпоставити, већ се мора пажљиво анализирати кроз кумулативне критеријуме из чл. 6, ст. 4 ГДПР, који укључују везу између сврха, контекст прикупљања и могуће последице по појединца.[34] Дакле, спојивост представља кључни тест који спречава алгоритамску експлоатацију корисничког поверења, будући да захтева да секундарна обрада остане у границама разумних очекивања појединца. У пракси ВИ, овај тест је често тешко доказив без претходне процене утицаја на заштиту података. Она представља процесни алат предвиђен чл. 35 ГДПР, који омогућава контролору (руковаоцу) да идентификује и ублажи ризике везане за обраду личних података. Процена утицаја на заштиту података је за системе ВИ суштински неопходна јер ови системи често укључују висок ризик због коришћења нових технологија и вршења систематског и обимног оцењивања личности путем аутоматизоване обраде.[35] Без овакве процене, начело ограничења сврхе постаје само „мртво слово на папиру” пред надирућом потребом алгоритама за новом аналитичком вредношћу, чиме се угрожава сама суштина информационог самоопредељења појединца.[36]

Централни стуб правне заштите грађана у ери свеприсутних алгоритама представља чл. 22 ГДПР, који прописује право појединца да не буде предмет одлуке донете искључиво на

[31] B. J. Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the “Right to Be Forgotten” in Big Data Practice*, Scripted, vol. 8, no. 3, 2011, 240.
[32] C. Kuner, L. Bygrave, K. Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, 308-312.
[33] European Data Protection Board (EDPB), *Guidelines 04/2019 on Article 25 Data Protection by Design and by Default*, op. cit., 19.
[34] European Data Protection Board (EDPB), *Guidelines 08/2020 on the Protection of Personal Data in the Context of the Use of AI*, 15–16, преузето 04.12.2025. https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf .
[35] R. Radu, *Negotiating Internet Governance*, Oxford University Press, Oxford, 2019, 89-91.
[36] M. Hildenbrandt, *op. cit.*, 92.

основу аутоматизоване обраде, укључујући профилисање, уколико та одлука производи правне последице по њега или на сличан начин значајно утиче на његов положај. У правној науци преовладава став да ово није само право које појединац треба да захтева активним деловањем, већ општа забрана аутоматизованог одлучивања која обавезује контролора (руковаоца), осим у три таксативно наведена изузетка: када је то неопходно за закључење или извршење уговора, када је прописано законом или на основу изричитог пристанка лица чији се податак обрађује.[37] Међутим, за дубље разумевање сукоба ВИ и права, неопходна је даља анализа тзв. права на објашњење. Овај концепт представља правни изазов јер сам термин „право на објашњење" није експлицитно уврштен у диспозицију чл. 22, већ се његови елементи изводе из Рецитала 71, који помиње право појединца да „добије објашњење одлуке донете након такве процене".[38] Доктринарни сукоб овде настаје између две струје. Док једни аутори заузимају став да право на објашњење постоји као интегрални део транспарентности, друга група аутора, заступа мишљење да ГДПР заправо не гарантује право на објашњење специфичне одлуке (нпр. „зашто је мени одбијен кредит?"), већ само право на информације о општој логици система (нпр. „који параметри утичу на оцену?").[39] Наведени јаз везује се за проблем тзв. црне кутије код неуронских мрежа, где је због комплекности математичких операција често немогуће пружити потпуну транспарентност. Тиме се ствара тензија између права на приватност и права на заштиту пословне тајне и интелектуалне својине програмера система. Начело транспарентности, утврђено у чл. 12 ГДПР, додатно компликује овај однос захтевајући да информације о обради буду пружене у сажетом, разумљивом и лако доступном облику. За системе ВИ ово значи обавезу пружања смислених информација о логици која се користи као и о значају и предвиђеним последицама такве обраде за испитаника. Изазов лежи у томе што „смисленост" информације зависи од примаоца па тако оно што је смислено инжењеру, просечном грађанину је потпуно неразумљиво. Контролор (руковалац) мора извршити демистификацију рада машине, што подразумева превођење алгоритамских процеса у јасан

[37] *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251rev.01, adopted on 3 October 2017, 19–21, преузето 7.12.2025. https://ec.europa.eu/newsroom/article29/items/612053 .
[38] Regulation (EU) 2016/679 (GDPR), *op. cit.*, Recital 71.
[39] S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, International Data Privacy Law, vol. 7, no. 2, 2017, 7–15.

језик који омогућава појединцу да разуме на основу којих главних критеријума је његов захтев одбијен, како би могао да оствари своје право на приговор.[40]

Из свега претходно наведеног произилази да ГДПР, иако технолошки неутралан, поставља строге оквире за примену ВИ кроз инсистирање на начелима минимизације и ограничења сврхе, чиме се директно супротставља природи алгоритамске експанзивности. Кључни изазов за савремено право остаје ефикасно спровођење права на објашњење и демистификација процеса аутоматизованог одлучивања, како би се заштитио дигнитет појединца пред нетранспарентношћу тзв. црних кутија система ВИ.

2.1. Акт о вештачкој интелигенцији – успостављање регулаторног оквира заснованог на ризику

Док је ГДПР фокусиран на заштиту података о личности као фундаментално право, Акт о вештачкој интелигенцији[41] представља *lex specialis* који регулише саме системе и њихов утицај на безбедност и основна права. Најзначајнија тачка преплитања ова два прописа лежи у покушају Европске Уније да коначно реши проблем тзв. црне кутије, који је у оквиру самог ГДПР остао на нивоу теоријске дебате у вези са правом на објашњење.

Акт о ВИ уводи строге обавезе транспарентности за системе високог ризика, чиме директно операционализује начела из члана 12 и 13 ГДПР. Према члану 13 Акта о ВИ, ови системи морају бити пројектовани и развијени на начин који обезбеђује да њихово функционисање буде довољно транспарентно како би субјекти могли да тумаче излазне резултате система. Наведно решење представља квалитативни помак са права да се добије информација ка разумвеању добијене информације. На тај начин, Акт покушава да премости јаз између правне норме и технолошке немогућности који је наишао на критику од стране

[40] L. Edwards, M. Veale, *Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For*, Duke Law & Technology Review, vol. 16, no. 1, 2017, 18–84.
[41] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on Artificial Intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), преузето 29.11.2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 .

научне јавности с обзиром на то да поједини аутори заступају мишљење да право на објашњење не може бити ефикасно ако дизајн алгоритма то не дозвољава. [42]

Посебно је значајна корелација у погледу управљања подацима. Члан 10, ст. 3 Акта о ВИ прописује да скупови података за обуку, валидацију и тестирање морају бити релевантни, репрезентативни и, колико је то могуће, без грешака и потпуни. Ово директно подупире начело тачности из чл. 5 ГДПР и проширује га на фазу која претходи самој обради података у реалном времену. Уколико систем ВИ учи на пристрасним или нетачним подацима о личности, он не само да крши ГДПР, већ према Акту о ВИ постаје неусклађен производ који не сме бити на тржишту Европке Уније. Акт о ВИ уводи „системски квалитет података" као законску категорију, чиме се спречава да алгоритми уче на дискриминаторним обрасцима који би касније резултирали повредом права појединца.Такође, Акт дозвољава обраду посебних категорија података тј. осетљивих података, као што су раса, етничко порекло и др., у сврху откривања и исправљања пристрасности тј. спречавања дискриминације, што представља специфичан законски основ који допуњује строге забране из чл. 9 ГДПР.[43]

Додатно, Акт о ВИ уводи концепт надзора од стране човека кроз чл. 14, који служи као директан технички коректив за чл. 22 ГДПР. Док ГДПР даје појединцу право да не буде предмет одлуке која је донета искључиво аутоматизовано, Акт о ВИ обавезује произвођаче да у систем угради механизме који омогућавају човеку да у сваком тренутку разуме, интервенише или искључи систем. Ово у пракси значи да људска интервенција (енг. *human in the loop*) не сме бити само пасивни посматрач, већ неко ко има стварну моћ да оспори алгоритамску одлуку на основу техничких параметара предвиђених Актом.

2.2. Системи високог ризика као фокусна тачка регулаторне контроле

У хијерархији коју успоставља Акт о ВИ, системи високог ризика представљају централну категорију на коју се односи највећи број императивних норми. За разлику од система минималног ризика, који су препуштени добровољним кодексима понашања, системи високог ризика су они који могу изазвати значајну штету по здравље, безбедност

[42] S. Wachter, B. Mittelstadt, *A Right to Reasonable Algorithmic Decision-Making: Unpacking Data Protection Law's Untapped Potential*, Columbia Business Law Review, 2019, 562–598.
[43] M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, Computer Law Review International, vol. 22, no. 4, 2021, 103.

или основна права грађана. Према чл. 6 Акта о ВИ, ова категорија обухвата две групе система: оне који се користе као безбедносне компоненте производа који већ подлежу трећој страни (нпр. медицински уређаји) и тзв. самосталне системе наведене у Анексу III, као што су системи за биометријску идентификацију, управљање критичном инфраструктуром, образовање и запошљавање.[44] Висок ризик често произлази управо из инвазивности обраде података о личности те би с тим у вези класификација система као високоризичног требало да буде сигнал контролорима (руковаоцима) да морају применити повишен степен пажње. У овом контексту, Акт о ВИ уводи строге захтеве за управљање ризиком кроз чл. 9, који захтева итеративни процес идентификације и ублажавања ризика током читавог животног циклуса система. Ова обавеза се директно преплиће са Проценом утицаја на заштиту података из ГДПР, док Процена утицаја на заштиту података анализира ризик по приватност појединца, систем управљања ризиком из Акта о ВИ анализира техничку поузданост и ширу друштвену безбедност система.[45] Додатно, чл. 27 Акта о ВИ уводи обавезу спровођења процене утицаја високоризичне АИ на основна права за одређене субјекте јавног сектора, што представља значајну допуну члану 35 ГДПР, јер приморава контролоре да анализирају не само заштиту података, већ и потенцијалну дискриминацију и утицај на људско достојанство.

Један од најзначајнијих изазова код система високог ризика јесте обезбеђивање квалитета скупова података за обуку алгоритама. Члан 10 Акта о ВИ поставља ригорозне стандарде који захтевају да подаци буду репрезентативни и без пристрасности, како би се спречили дискриминаторни исходи у областима попут кредитног бодовања или софтвера за запошљавање. Нарочита пажња посвећена је биометријским системима наведеним у тачки 1. Анекса III, где обрада посебних категорија података из чл. 9 ГДПР, а која се између осталог односи и на генетске и биометријске податке, постаје извор високог ризика због могућности масовног надзора и идентификације појединаца без њиховог знања.[46] Поједини аутори истичу да оваква регулација високог ризика представља покушај права да очува људску

[44] Annex III: *High-Risk AI Systems Referred to in Article 6(2)*, преузето 01.12.2025, https://artificialintelligenceact.eu/annex/3/.
[45] M. Ebers, *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in: L. DiMatteo, C. Poncibo, M. Cannarsa (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, Cambridge, 2021, 330.
[46] F. J. Zuiderveen Borgesius, *Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence*, The International Journal of Human Rights, vol. 24, no. 10, 2020, 1572–1593.

аутономију у ситуацијама када су одлуке машина од егзистенцијалног значаја за појединца.[47]

У завршници, за системе високог ризика предвиђена је обавеза креирања детаљне техничке документације и вођења аутоматских записа о раду система што омогућава накнадну контролу и утврђивање одговорности у случају инцидента. Према чл. 12 Акта о ВИ, ови записи морају омогућити праћење функционисања система током његовог животног века, што директно олакшава доказивање усклађености са начелом транспарентности из ГДПР. Ово је инструмент који омогућава остваривање начела одговорности из чл. 5, ст. 2 ГДПР, претварајући теоријску обавезу контролора у опипљив технички доказ који надзорни органи могу верификовати. Такође, чл. 86 Акта о ВИ даје право појединцима да захтевају јасно и разумљиво објашњење улоге ВИ система у поступку доношења одлука које на њих значајно утичу, чиме се коначно нормативизује доктринарно право на објашњење које је у оквиру ГДПР било спорно.

2.3. Упоредна анализа Опште уредбе о заштити података и Акта о ВИ

Упоредна анализа ГДПР и Акта о ВИ открива релацију супсидијарности и комплементарности, при чему ова два прописа заједно чине ригорозан регулаторни оквир. Док је ГДПР примарно усмерена на заштиту субјективитета појединца кроз контролу обраде података о личности, Акт о ВИ се фокусира на безбедност и поузданост самог технолошког производа и његовог животног циклуса. Ова дистинкција је кључна јер ГДПР регулише „улаз" података, док Акт о ВИ ставља фокус на „излаз" и техничке перформансе алгоритма.[48] Овим се ствара интегрални штит који штити грађанина не само од злоупотребе информација, већ и од материјалних и моралних последица неисправног рада паметних система.

Кључна тачка конвергенције је концепт одговорности. Према чл. 5, ст. 2 ГДПР, контролор (руковалац) сноси терет доказивања усклађености са начелима обраде, али Акт о ВИ ову обавезу конкретизује кроз чл. 11 и 12, захтевајући вођење непрекидног техничког дневника

[47] K. Yeung, *Why Worry About Decision-Making by Machine?*, in: K. Yeung, M. Lodge (eds.), *Algorithmic Regulation*, Oxford University Press, Oxford, 2019, 32.
[48] C. Kuner, L. Bygrave, K. Docksey, op. cit., 312.

и креирање документације која омогућава накнадну ревизију алгоритамских процеса. Ово у пракси значи да је начело одговорности из ГДПР коначно добило свој технички „инструментаријум", чиме се онемогућава оправдање контролора да је алгоритамска одлука „необјашњива" због своје комплексности.[49] Друга важна тачка је процесно управљање ризиком. Док Процена утицаја на заштиту података из члана 35 ГДПР мапира специфичне опасности по приватност, систем управљања ризиком из чл. 9 Акта о ВИ захтева од провајдера да предвиде и сузбију шире друштвене ризике, укључујући системску дискриминацију и утицај на здравље грађана.

Најзначајнији нормативни помак остварен је у домену права на објашњење. Акт о ВИ у чл. 86 даје појединцу изричито право на објашњење улоге система у поступку доношења одлука које на њега производе правне последице, чиме се решава доктринарна недоумица око домета Рецитала 71 ГДПР. Ова нормативна интеграција директно се надовезује на чл. 13 Акта о ВИ, који прописује да транспарентност мора бити таквог нивоа да омогући кориснику разумевање начина рада система, чиме се пословна тајна програмера ставља у други план у односу на јавни интерес заштите основних права.

Дакле, можемо закључити да Акт о ВИ није замена за ГДПР, већ исти суштински подиже на виши ниво и то техничким стандардима без којих би заштита приватности у дигиталном добу остала само декларативна категорија.

[49] L. A. Bygrave, *Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decision-Making*, in: M. Ienca, O. Pollicino, L. Liguori, E. Stefanini, R. Andorno (eds.), *Information Technology, Life Sciences and Human Rights*, Cambridge University Press, Cambridge, 2022, 170.

III ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ У ПРИМЕНИ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У РЕПУБЛИЦИ СРБИЈИ

С обзиром на то да у овом раду анализирамо заштиту података о личности с аспекта примене ВИ то је потребно предметну анализу усмерити и на правни систем Републике Србије. Стога ћемо прво указати на развој заштите податак о личности на нашем подручју, а након тога дефинисати основне стубове на којима ова симбиоза почива. ВИ не постоји у правном вакууму, већ је њена суштина нераскидиво везана за масовну обраду података, од којих значајан део, по својој природи и ефектима, потпада под режим заштите података о личности. С тим у вези у овом делу рада анализираћемо чланове Закона о заштити података о личности за које сматрамо да се могу довести у везу са ВИ као новим субјектом обраде.

1. Развој заштите података о личности у домаћем праву

Посматрано из историјске перспективе, интензивирање потребе за правном регулативом у сфери заштите података о личности везује се за другу половину 20. века, што је у директној корелацији са експанзијом савремених комуникационих технологија. У домаћем правном систему, специфично у оквиру тадашње Савезне Републике Југославије, овај институт је први пут експлицитно конституционализован Уставом из 1992. године[50]. Одредбама члана 33. поменутог највишег правног акта постављени су темељи заштите информационог интегритета појединца. Поред опште гаранције неповредивости личних података, уставне норме су предвиделе и стриктну забрану сврсисходног одступања, односно коришћење података супротно примарној намени прикупљања. Такође, појединцима је зајемчено право на информисаност о прикупљеним записима који се на њих односе, уз обезбеђивање механизма судске заштите у ситуацијама када дође до противправне употребе или злоупотребе тих информација.

Даљи искорак у нормативном утемељивању ове материје остварен је доношењем Закона о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних

[50] Устав Савезне Републике Југославије, *Службени лист СРЈ*, бр. 1/92.

података[51]. Овом ратификацијом у унутрашњи правни поредак имплементирани су стандарди истоименог међународног акта из 1981. године, чиме је успостављен примарни циљ заштите који се везује за осигуравање поштовања темељних слобода и права сваког физичког лица на територији државе уговорнице. Посебан фокус Конвенције усмерен је на заштиту права на приватност у контексту компјутеризоване обраде информација, при чему су ове гаранције универзалног карактера и не зависе од држављанства или пребивалишта субјекта на кога се подаци односе.[52]

Сходно уставном овлашћењу из члана 33. става 4. Устава СРЈ, којим је предвиђено да се материја прикупљања, обраде и заштите информација о појединцу дефинише посебним законским актом,[53] јавила се неопходност за детаљнијим правним уобличавањем ове сфере. Као одговор на ту потребу, 1998. године усвојен је први Закон о заштити података о личности[54], који је кроз релативно сажет корпус од 27 чланова поставио елементарне оквире регулације. Ипак, овај нормативни акт патио је од одређених мањкавости, првенствено због неусклађености са тадашњим европским правним стандардима и немогућности да адекватно одговори на изазове које је наметнуо нагли технолошки прогрес. Такве околности наметнуле су потребу за креирањем модернијег законског решења које би било синхронизовано са савременим друштвеним и техничким трендовима.

Следећи Закон о заштити података о личности[55] настао је као одговор у процесу усклађивања српског законодавства са законодавством Европске уније, посебно са Дитективом 95/46/ЕЦ која је тада била на снази. Будући да је важећи Закон о заштити података личности креиран у складу са поменутом Директивом то и не чуди што је материја детаљније уређена па је тако прописана јача улога Повереника за информације од јавног значаја и заштиту података о личности, а поред наведеног уведени су строжи критеријуми када је у питању сама материја на коју се Закон и односи. Наведеним Законом, домаће законодавство је по први пут прецизно концептуализовало термин податак о личности.

[51] Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података, Службени лист СРЈ – Међународни уговори, бр. 1/92.
[52] Д. Гајић, *Заштита података о личности према Уставу СРЈ и предлогу закона о заштити података о личности*, Гласник Адвокатске коморе Војводине, вол. 68, бр. 9, 1996, стр. 349.
[53] Устав СРЈ, чл. 33, ст. 4.
[54] Закон о заштити података о личности, *Службени лист СРЈ*, бр. 24/98.
[55] *Службени гласник РС, бр. 97/2008, 104/2009 – други закон, 68/2012 – одлука УС и 107/2012.*

Према овом законском решењу, предметни појам обухвата сваку информацију која се може довести у везу са физичким лицем, при чему је потпуно ирелевантан медијум на којем је она забележена (било да је реч о аналогним форматима попут папира и филма или савременим електронским записима). Дефиниција је постављена изузетно широко, тако да обухвата податке независно од њиховог порекла, начина на који се до њих дошло (непосредним опажањем или увидом у документацију), места њиховог депоновања, као и субјекта који управља њиховим складиштењем. Овакав свеобухватан приступ омогућио је да свако својство информације, без обзира на техничке или формалне карактеристике, потпадне под режим заштите уколико је идентитет лица одредив.[56]

У тежњи ка хармонизацији са европским правним тековинама усвојен је важећи Закон о заштити података о личности[57], који у великој мери представља рецепцију решења из ГДПР. Овај нормативни акт на бухватан и детаљан начин инкорпорира савремене стандарде информационе приватности у домаћи поредак. Поред законске материје, заштита личних података ужива и највиши степен правног дејства, будући да је експлицитно зајемчена одредбама актуелног Устава Републике Србије у оквиру корпуса људских права и основних слобода.[58] Важно је истаћи да је предметна материја додатно нормирана кроз екстензиван корпус *lex specialis* који специфично уређују заштиту података унутар појединих ресора. Тако се, поред општег правног оквира, примена правила о заштити приватности модификује и конкретизује кроз прописе као што су Закон о слободном приступу информацијама од јавног значаја[59], који успоставља баланс између транспарентности и приватности, те Закон о здравственој документацији и евиденцијама у области здравства[60], који штити нарочито осетљиве категорије података. Сличну улогу имају и акти који регулишу радне односе[61], матичне књиге[62], електронске комуникације[63] и информациону безбедност[64] као и други закони, чиме се ствара комплексан и кохерентан систем заштите личних информација у свим

[56] Ibid., чл. 3, ст. 1, тачка 1.
[57] *Службени гласник РС*, бр. 87/2018.
[58] Устав Републике Србије, *Службени гласник РС*, бр. 98/2006 и 115/2021, чл. 42. ст. 1.
[59] *Службени гласник РС*, бр. 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021.
[60] *Службени гласник РС*, бр. 92/2023.
[61] Закон о раду, *Службени гласник РС*, бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 – одлука УС, 113/2017, 95/2018 – аутентично тумачење и 109/2025 - др. Закон.
[62] Закон о матичним књигама, *Службени гласник РС*, бр. 20/2009, 145/2014 и 47/2018.
[63] Закон о електронским комуникацијама, *Службени гласник РС*, бр. 44/2010, 60/2013 – одлука УС, 62/2014, 95/2018 – др. Закон и 35/2023 – др. Закон.
[64] Закон о информационој безбедности, *Службени гласник РС*, бр. 91/2025.

сегментима друштвеног деловања. Поред законских оквира, нормативна инфраструктура заштите података о личности обухвата и екстензиван корпус подзаконских аката, који имају нижу правну снагу, али кључну улогу у операционализацији прописа. Ови акти, попут специфичних правилника професионалних асоцијација или техничких прописа о вођењу евиденција о лицима задуженим за заштиту података, омогућавају прецизну примену општих законских начела у пракси. Такође, стратешко усмерење ове области дефинисано је дугорочним развојним документима, као што је Стратегија заштите података о личности за период од 2023. до 2030. године[65], којом се постављају приоритети и циљеви за даље унапређење институционалног оквира и подизање нивоа заштите права грађана.

2. Закон о заштити података о личности и примена вештачке интелигенције

У циљу обухватног сагледавања заштите података о личности и примене вештачке интелигенције у овом делу рада посебну пажњу ћемо посветити начелима обраде података, законитости обраде, обради посебних врста података, праву на ограничење обраде, аутомстском доношењу појединачних одлука и профилисању, мерама заштите, безбедноцти обраде података, процени уицаја на заштиту података као и претходном мишљењу Повереника.

2.1. Начела обраде података у примени вештачке интелигенције

У ери експанзије вештачке интелигенције, члан 5. Закона о заштити података о личности (у даљем тексту: ЗЗПЛ), који се односи на начела обраде података, представља примарни нормативни филтер кроз који сваки систем машинског учења мора проћи. Иако су начела дефинисана технолошки неутрално, њихова апликација у контексту тзв. великих података суочава се са озбиљним доктринарним изазовима. С тим у вези начело законитости, правичности и транспарентности[66] представља темељни стуб заштите података о личности, обједињујући три суштинска аспекта којима се осигурава интегритет обраде у односу на

[65] *Службени гласник РС*, бр. 72/23.
[66] ЗЗПЛ, чл. 5, ст. 1, тачка 1.

појединца. Првенствено, захтев за законитошћу подразумева да се свака операција прикупљања или обраде података мора строго заснивати на једној од таксативно наведених правних основа из ЗЗПЛ, као што су изричити пристанак лица, извршење уговорних или законских обавеза, заштита виталних интереса или легитимни интерес руковаоца.[67] Уско повезано са законитошћу је и начело правичности којим се захтева да обрада буде заснована на високој професионалној етици и савесности, уз дужно поштовање интереса лица на која се подаци односе.[68] Да одсуство ових вредности може бити санкционисано, илуструје случај компаније Тик-ток, којој је 2023. године изречена казна од 345 милиона евра управо због симултаног кршења принципа законитости, правичности и транспарентности.[69] Овакав пример јасно указује на чињеницу да формално поседовање правног основа није довољно уколико сама обрада нарушава етичке стандарде заштите приватности. Коначно, принцип транспарентности обавезује руковаоце да појединцима пруже јасне, потпуне и лако доступне информације о сврси, начину и правном основу обраде њихових података. Актуелни изазови у домаћој пракси, попут поступања компанија Мета и X Corp, додатно наглашавају значај овог начела. Чињеница да је Мета у јуну 2024. године применила измењену политику приватности у Републици Србији без претходног обавештавања корисника, док је, с друге стране у Европској унији иста пракса обустављена након бурних реакција указује на изражену правну неједнакост.[70] Овакви примери селективне транспарентности и редефинисања правних основа, где се легитимни интерес користи као супституит за пристанак без адекватне информисаности, представљају озбиљну препреку у остваривању потпуне заштите права грађана у дигиталном окружењу. Транспарентност је можда највећи камен спотицања за системе ВИ засноване на дубоком учењу. Проблем тзв. црне кутије онемогућава потпуно разумевање начина на који алгоритам долази до одређеног

[67] Ibid., чл. 12.
[68] С. Гајин, *Заштита података о личности у сектору безбедности: водич кроз законску регулативу*, Центар за унапређивање правних студија; Организација за европску безбедност и сарадњу, Мисија ОЕБС-а у Србији, Београд, 2019, 13.
[69] У овом случају радило се о прикупљању личних података регситрованих корисника коју су или млађи од 13 година или су у старосној доби између 13 и 17 година. The Data Protection Commission, *Binding Decision 2/2023 on the Dispute Submitted by the Irish SA regarding TikTok Technology Limited*, 1 September 2023, преузето 10.01.2026, https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en.
[70] Share фондација, *Мета променила политику приватности: Наши подаци као материјал за тренинг АИ*, преузето 11.01.2026, https://sharefoundation.info/meta-promenila-politiku-privatnosti-nasi-podaci-kao-materijal-za-trening-ai/.

решења.[71] Са аспекта ЗЗПЛ, „поштење" подразумева да обрада не сме бити обмањујућа или дискриминаторна.[72] Уколико систем користи прикривене пристрасности које резултирају индиректном дискриминацијом одређених група грађана, таква обрада је супротна начелу поштења.[73] Транспарентност у у случају овог начела подразумева право лица да разуме логику и последице обраде.

Уско повезано са претходним јесте и начело ограничења сврхе, које налаже да се подаци прикупљају искључиво за конкретно дефинисане и легитимне намене.[74] Свака даља обрада изван тих оквира забрањена је уколико не постоји нови правни основ или ако корисници нису упознати са новом сврхом. Примера ради, подаци о физичкој конституцији путника које прикупља авио-компанија ради распореда седишта не могу се накнадно достављати имиграционим службама без релевантног законског утемељења.[75] Ипак, када је у питању начело ограничења сврхе постоје изузеци у случајевима архивирања, научног, историјског или статистичког истраживања, под условом да се тиме не угрожавају основна права појединаца.[76]

Начело минимизације података предвиђа да прикупљене информације морају бити примерене, релевантне и строго ограничене на оно што је неопходно за остваривање конкретне сврхе обраде.[77] У пракси, ово начело спречава прекомерно задирање у приватност појединца где би нам као пример могао послужити извештај о привременој спречености за рад који се доставља послодавцу ради обрачуна накнаде зараде а који не сме садржати дијагнозу или шифру болести, јер ти подаци нису неопходни приликом обрачуна накнаде

[71] S. Wachter, B. Mittelstadt, C. Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, Harvard Journal of Law & Technology, vol. 31, no. 2, 2018, 842–887.
[72] M. Vitajić, Ethical and Practical Challenges of Artificial Intelligence (AI) in Legal Practice and Judiciary; in: Matić Bošković, M. Kostić, J (ed.), *Shaping Justice:How Penal Law and Judiciary Address Contemporary Societal Challenges*, Belgrade, 2025, Institute of Comparative Law, Institute of Criminological and Sociological Research, Judical Academy, 111.
[73] European Commission for the Efficiency of Justice (CEPEJ), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment*, Council of Europe, 2018, 9, преузето 17.12.2025, https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf.
[74] ЗЗПЛ, чл.5, ст. 1, тачка 2.
[75] Агенција Европске уније за основна права и Савет Европе, *Приручник о европском праву заштите података*, Агенција Европске уније за основна права и Савет Европе, Луксембург, 2018, стр. 124, преузето 11.01.2026, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_sr.pdf.
[76] С. Андоновић, Д. Прља, *op. cit*., 67.
[77] ЗЗПЛ, чл. 5. ст. 1, тачка 3.

зараде.[78] Један од кључних механизама за практичну примену овог начела јесте псеудонимизација, поступак којим се директни идентификатори замењују алтернативним подацима, попут иницијала. Овај метод се редовно примењује приликом јавног објављивања судских пресуда, чиме се обезбеђује равнотежа између транспарентности правосуђа и заштите идентитета учесника у поступку.[79] Сагледавањем ВИ кроз призму начела заштите података, конкретно корз начело минимизације и ограничења сврхе, уочавамо да је један од највећих парадокса ВИ њен интроспективни карактер будући да се системи често тренирају на огромним сетовима података како би се открили корелације које у тренутку прикупљања нису биле предвидиве. С тим у вези, начело ограничења сврхе захтева да подаци буду прикупљени за конкретне, јасне и легитимне сврхе. Системи ВИ често су неодвојиви од феномена ширења података, где се подаци прикупљени у једну сврху накнадно користе за тренирање потпуно других алгоритама, што може довести до повреде овог начела уколико не постоји компатибилност сврха.[80]

Начело тачности података обавезује руковаоце да осигурају прецизност информација које обрађују, уз претпоставку да се нетачни подаци морају без одлагања избрисати или исправити.[81] Према ставу Повереника, за испуњење овог начела није довољно само декларативно навођење обавеза у општим актима, већ је руковалац дужан да примени конкретне организационе, техничке и кадровске мере. То подразумева прецизно дефинисање радњи које запослени морају предузети како би се осигурала поузданост података, чиме се спречава неоправдано пребацивање одговорности на појединце унутар система.[82] Ипак, примена овог начела зависи од природе саме обраде. Док је у већини случајева ажурирање императив, постоје ситуације у којима је оно недопустиво ради очувања веродостојности записа. Типичан пример је медицинска документација о извршеној хируршкој интервенцији или подаци који служе документовању историјских догађаја, где би накнадна измена нарушила чињенично стање забележено у тренутку

[78] Предмет бр. 073-14-2819/2021-02 од 02.11.2021. године, *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, публикација бр. 7, Београд, 2022,179.
[79] Агенција Европске уније за основна права и Савет Европе, *op. cit*., 128.
[80] M. Vitajić, *op. cit*., 108.
[81] ЗЗПЛ, чл. 5, ст. 1, тачка 4.
[82] Предмет бр. 072-07-2076/2020-07 од 05.10.2020. године, *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, публикација бр. 7, Београд, 2022, 31.

настанка документа.[83] Начело тачности у контексту ВИ не односи се само на фактографску исправност улазних података, већ и на репрезентативност података којима се алгоритам тренира. Коришћење пристрасних или непотпуних сетова података доводи до алгоритамске дискриминације и „халуцинација" система.[84] ЗЗПЛ обавезује руковаоца да предузме све разумне мере како би се нетачни подаци избрисали или исправили, што у сложеним неуронским мрежама постаје технички изазов будући да се односи на право на заборав унутар модела.

Начело интегритета и поверљивости, обавезује руковаоце да осигурају свеобухватну заштиту података током целог процеса обраде. Циљ је спречити било какав облик неовлашћеног приступа, незаконите употребе, али и случајне губитке или физичка оштећења информација. Да би се овај стандард испунио, неопходно је спровести скуп техничких, организационих и кадровских мера које заједно чине сигурносни штит око личних података.[85] У пракси се за очување поверљивости најчешће користе методе попут псеудонимизације и криптозаштите. Док псеудонимизација онемогућава директну идентификацију лица без додатних информација, криптозаштита (шифровање) обезбеђује да подаци постану потпуно нечитљиви за неовлашћене субјекте. Овакви механизми су кључни за одржавање високог нивоа приватности, чак и у ситуацијама када дође до безбедносних инцидената.

Суштина начела ограничења чувања[86] података огледа се у обавези руковаоца да личне податке у идентификујућем облику задржава искључиво током периода који је неопходан за реализацију конкретне сврхе обраде.[87] *Ratio legis* оваквог ограничења је двосмеран. С једне стране, примарно се тежи минимизацији ризика од злоупотребе података, док се истовремено подиже ефикасност самог система кроз рационализацију трошкова и ресурса.[88] Иако регулатива предвиђа одређене изузетке,превасходно када је реч о заштити јавног

[83] Агенција Европске уније за основна права и Савет Европе, *op. cit*., 130.
[84] Ibid., 109.
[85] ЗЗПЛ, чл. 5, ст. 1, тачка 6.
[86] Колико је ово правило обавезујуће у пракси, илуструје интервенција Повереника у случају једног факултета. Установа је санкционисана јер није успоставила адекватне рокове нити заштитне мере, чиме је омогућено да се подаци лица чувају знатно дуже него што је то природа образовне делатности захтевала. Предмет бр. 072-04-296/2021-07 од 26.02.2021. године, *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, публикација бр. 7, Београд, 2022, 164.
[87] ЗЗПЛ, чл. 5, ст. 5.
[88] С. Андоновић, Д. Прља, *op. cit*., 71.

интереса или архивским сврхама, важно је нагласити да чак ни у тим околностима закон не дозвољава неограничено и произвољно задржавање информација. Сваки временски оквир мора бити оправдан и пропорционалан циљу који се жели постићи.[89] Вештачка интелигенција тежи дуготрајном задржавању података ради континуираног побољшања перформанси, што је у директној супротности са начелом да се подаци чувају само онолико колико је потребно за остваривање сврхе. Такође, интегритет и поверљивост су изложени новим врстама сајбер претњи, што захтева виши степен техничких мера заштите предвиђених законом.

Начело одговорности представља круну система заштите података, јер обавезује руковаоца не само на примену свих претходно наведених принципа, већ и на активну способност доказивања те усклађености. То подразумева континуирано спровођење адекватних мера, попут псеудонимизације и других заштитних механизама, како би се осигурао интегритет обраде у сваком тренутку.[90] Специфичност овог начела је у томе што руковалац мора бити проактиван с обзиром на то да је дужан да доказује своју компетентност у заштити приватности независно од тога да ли су покренути надзорни поступци или иницијативе самих грађана.[91] Сваки појединац чија су права повређена има законску могућност подношења тужбе за накнаду штете, што додатно оптерећује одговорно лице. Ово начело пребацује терет доказивања на руковаоца. У комплексним екосистемима ВИ, где често учествује више актера, начело одговорности захтева јасан папиролошки и технички след. Руковалац у Републици Србији мора бити у стању да у сваком тренутку демонстрира Поверенику да је његов ВИ модел усклађен са свим претходно наведеним начелима. Ово подразумева вођење детаљних евиденција о обради и имплементацију робусних интерних политика управљања подацима.

2.2. Законитост обраде и примена вештачке интелигенције

[89] Ibid.
[90] ЗЗПЛ, чл. 5, ст. 2, чл. 42.
[91] Агенција Европске уније за основна права и Савет Европе, *op. cit*., 139.

Члан 12. ЗЗПЛ представља камен темељац законитости обраде, прописујући да је обрада допуштена искључиво уколико је испуњен најмање један од таксативно наведених правних основа. Ови основи обухватају следеће: изричит пристанак лица на које се подаци односе[92], неопходност обраде за извршење уговора[93], испуњење законских обавеза руковаоца[94], заштиту животних интереса[95], обављање послова у јавном интересу или вршење службених овлашћења[96], те легитимни интерес руковаоца или треће стране[97].

Законитост обраде података о личности, у смислу ЗЗПЛ, подразумева да руковалац у сваком конкретном случају изабере одговарајући правни основ у складу са околностима обраде. Међутим, законитост се не исцрпљује у самом избору правног основа, већ обухвата и поштовање начела обраде из чл. 5. ЗЗПЛ, као и испуњавање свих прописаних обавеза, попут вођења евиденције обраде, именовања лица за заштиту података и омогућавања остваривања права лица на које се подаци односе. Дакле, обрада је законита само ако је испуњен један од законом прописаних услова, укључујући и случај када је обрада неопходна ради остваривања легитимних интереса руковаоца или треће стране, под условом да ти интереси не превагну над правима и слободама лица на које се подаци односе.[98] Да би се легитимни интерес сматрао ваљаним правним основом, морају бити испуњени следећи услови: постојање легитимног интереса, неопходност обраде и претежност тог интереса у односу на права и слободе лица. Овај основ се не може примењивати аутоматски, већ је потребно унапред утврдити испуњеност наведених услова. У циљу обезбеђивања начела законитости, транспарентности и одговорности, руковалац је дужан да документује процену испуњености ових услова. Иако закон не прописује обавезну форму, препоручује се израда

[92] ЗЗПЛ, чл. 12, ст. 1, тачка 1.
[93] Ibid., тачка 2.
[94] Ibid., тачка 3.
[95] Ibid., тачка 4.
[96] Ibid., тачка 5.
[97] Ibid., тачка 6.
[98] Повереник за информације од јавног значаја и заштиту података о личности, *Легитимни интерес као правни основ за обраду података о личности*, преузето 27.12.2025, Legitimni interes kao pravni osnov za obradu podataka o ličnosti - Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti.

писаног акта о процени легитимног интереса пре отпочињања обраде.[99]Уколико је руковалац већ израдио акт о процени утицаја обраде, није потребно доносити посебан акт о процени легитимног интереса, јер тај документ већ садржи релевантне елементе, укључујући и опис легитимног интереса. Први корак у процени применљивости легитимног интереса као правног основа јесте утврђивање конкретног циља намераване обраде, односно користи која се њоме жели постићи за руковаоца, трећу страну или ширу јавност. Тај циљ мора бити правно допуштен и у складу са професионалним стандардима, а руковалац је дужан да га прецизно дефинише, без ослањања на опште формулације пословног интереса.[100] При томе, требало би узети у обзир да појам легитимног интереса представља шири концепт од саме сврхе обраде. Да би услов неопходности био испуњен, обрада мора бити нужна за остварење постављеног циља. Уколико се исти циљ може постићи без обраде података о личности или уз мање инвазивне мере, овај услов није испуњен. Интензитет задирања у приватност директно утиче на процену ризика по права и слободе лица. Поред тога, потребно је оценити да ли лице на које се подаци односе може разумно очекивати такву обраду у датим околностима, имајући у виду да неочекивана обрада може довести до губитка контроле над подацима и отежаног остваривања права.[101] Такође, руковалац је дужан да процени потенцијалне последице обраде по права и слободе лица, укључујући право на приватност и заштиту података, али и друга основна права. Ова процена обухвата идентификацију могућих извора ризика, као и анализу вероватноће и тежине штетних последица (материјалних и нематеријалних), које могу проистећи из различитих околности обраде, као што су техничка средства, начин обраде, приступ подацима и шири друштвени контекст.[102] На основу процене вероватноће настанка ризика и озбиљности могуће штете, утврђује се ниво ризика по права и слободе лица (нпр. низак, умерен или висок). Полазећи од тако добијених резултата, руковалац је дужан да оцени да ли је заштита права лица пропорционална очекиваној користи обраде. Уколико потенцијална штета превазилази корист, легитимни интерес неће представљати адекватан правни основ. У случају обраде засноване на легитимном интересу, лице има право да у сваком тренутку уложи приговор. Тада руковалац мора обуставити обраду, осим ако докаже

[99] Ibid.
[100] Ibid.
[101] Ibid.
[102] Ibid.

постојање претежних законских разлога или потребу за остваривање, заштиту или одбрану правног захтева. Ако се приговор одбије, руковалац је у обавези да образложи такву одлуку и обавести лице о праву на подношење притужбе надлежном органу или тужбе суду. Овакав правни режим захтева повећан степен опреза при ослањању на легитимни интерес као основ обраде.[103]

У контексту ВИ, предметни члан престаје да буде само формални захтев и постаје поље сукоба између технолошког детерминизма и права на информационо самоопредељење. Највећи изазов представља тзв. секундарна обрада података. Док се традиционални системи базирају на линеарној обради, модели ВИ функционишу на принципу рекурзивног учења, где се подаци прикупљени за једну сврху (нпр. услуга е-трговине) користе за тренинг сложених неуронских мрежа чији крајњи исходи често нису предвидиви у тренутку прикупљања.[104] Иако се пристанак често сматра најјачим основом, код система ВИ он се суочава са кризом валидности. Да би пристанак био пуноважан, он мора бити добровољан, конкретан, информисан и недвосмислен. Међутим, због феномена тзв. црне кутије, руковаоци често нису у могућности да пруже потпуну информацију о томе како ће алгоритам користити податке у будућности, што води ка тзв. парадоксу приватности будући да корисници дају пристанак на комплексе услове коришћења које не разумеју, чиме се обесмишљава заштитна функција овог члана.[105] За компаније које развијају ВИ, легитимни интерес је најфлексибилнији, али и најризичнији основ. За његову примену неопходно је кумулативно испуњење три теста: теста сврхе који се везује за постојање легитимног интереса, теста неопходности што значи да обрада мора бити неопходна за остварење тог интереса и теста равнотеже који подразумева постојање баланса интереса руковаоца са правима лица. У вези са наведеним сматра се да масовно прикупљање података са интернета ради тренинга великих језичких модела тешко може проћи трећи тест тј. тест равнотеже, јер појединци чији се подаци прикупљају нису могли разумно очекивати такву врсту обраде.[106]

[103] Ibid.
[104] F.Z. Borgesius, *Discrimination, Arteficial Intelligence and Algorithmic*, Council of Europe, Strasbourg, 2018, 11-15
[105] S. Watcher, B. Mittelstadt, C. Russel, *op. cit*., 846-850.
[106] European Data Protection Board (EDPB), *Report of the Work Undertaken by the ChatGPT Taskforce*, 6, преузето 30.01.2026, https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf.

Сходно наведеном, примена чл. 12 ЗЗПЛ у сфери ВИ не сме се тумачити као технолошка препрека, већ као неопходан правни коректив који осигурава да економски интерес развоја алгоритама не превлада над фундаменталним правом појединца на информационо самоопредељење.

2.3. Обрада посебних врста података о личности и примена вештачке интелигенције

Члан 17. ЗЗПЛ дефинише посебне категорије података који, због своје интимне природе и потенцијала за дискриминацију, уживају висок степен правне заштите. Нормативна структура овог члана заснива се на општој забрани обраде података који откривају расно или етничко порекло, политичко мишљење, верска или филозофска уверења, као и чланство у синдикату. Надаље, забрана се експлицитно протеже на генетичке и биометријске податке уколико се они обрађују у сврху јединствене идентификације лица, као и на податке о здравственом стању, сексуалном животу или сексуалној оријентацији (ст.1). Дакле, претходно наведене податке је забрањено обрађивати осим када се ради о изузеним случајевима који се везују за животни интерес оних лица чији се подаци обрађују или када су ти подаци од значаја за јавни интерес.[107]С тим у вези законодавно решење у ст. 2. овог члана предвиђа десет таксативно наведених изузетака којима се ова забрана дерогира. Најрелевантнији изузеци за развој и примену система вештачке интелигенције обухватају изричит пристанак лица (тачка 1), обраду неопходну за извршење обавеза руковаоца у области социјалног осигурања и социјалне заштите (тачка 2), заштиту животних интереса лица (тачка 3), као и обраду која је неопходна из разлога значајног јавног интереса утврђеног законом (тачка 7). Специфичност овог члана лежи у томе што он не дозвољава редовне правне основе попут легитимног интереса, већ захтева знатно строже оправдање за сваку интервенцију у ову заштићену сферу.

У српском правном систему, овај члан представља неприкосновено језгро приватности. Из тог разлога Стратегија развоја вештачке интелигенције у Републици Србији за период 2025-2030. године препознаје значај ових података за развој сектора медицине и

[107] М. Кузминац, *Заштита података о личности: питање будућности које је „предухитрила“ садашњост*, Правни записи, вол. XV, бр. 2, 2024, 567.

персонализованих услуга, али истовремено наглашава неопходност примене највиших стандарда заштите. Такође, Етичке смернице за развој, примену и употребу поуздане и одговорне вештачке интелигенције (у даљем тексту: Етичке смернице)[108] инсистирају на томе да примена ВИ над осетљивим подацима мора бити праћена строгом људском контролом како би се спречила аутоматизована дискриминација.

Примена система ВИ суштински мења парадигму заштите посебних врста података из предметног члана, трансформишући их из пасивних информација у активне параметре за алгоритамско одлучивање. Овај процес је нарочито значајан када говоримо о биометријском надзору и алгоритамској пристрасности. Примена софтвера ВИ за препознавање лица на јавним просторима представља најекстремнији облик обраде биометријских података у сврху јединствене идентификације лица. Иако се ова технологија често оправдава јавним интересом или националном безбедношћу[109], ипак, можемо поставити питање да ли су опште одредбе ЗЗПЛ довољан и адекватан правни основ за овако инвазивну и неселективну обраду. Проблем се огледа у чињеници да системи ВИ прикупљају биометријске векторе свих лица у видном пољу камере, без обзира на постојање сумње, чиме се анонимност у јавном простору *de facto* укида[110] о чему би без сваке сумње требало водити рачуна приликом креирања законодавног оквира који се односи на употребу ВИ. Најопаснији аспект модерних модела ВИ је њихова способност да путем анализе наизглед неутралних података (нпр. дигитални отисци, историја претраге, брзина кретања курсора) са високим степеном тачности изведу закључак о посебним категоријама података.[111] Примера ради, алгоритам може предвидети здравствено стање корисника (депресију или хроничне болести) пре него што је самом кориснику постављена дијагноза[112], или закључити о његовој сексуалној оријентацији на основу образаца понашања на мрежама[113]. Овај феномен ствара правни вакуум будући да руковалац тврди да не обрађује осетљиве податке

[108] *Службени гласник РС*, бр. 23/23.
[109] ЗЗПЛ, чл. 17, ст. 2, тачка 7.
[110] European Data Protection Board (EDPB), *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, 10–11, преузето 11.01.2026, https://www.edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.
[111] S. Wachter, B. Mittelstadt, *op. cit*., 570-573.
[112]S. Wachter, *The Theory of Artificial Immutability: Protecting Algorithmic Groups under Anti-Discrimination Law*, Tulane Law Review, vol. 97, no. 2, 2023, 21–26.
[113] A. M. Kristen, J. Ugander, *Monophily in Social Networks Introduces Similarity among Friends-of-Friends*, Nature Human Behaviour, vol. 2, no. 4, 2018, 284.

јер их није прикупио изворно, док алгоритам суштински врши дискриминацију на основу тих изведених категорија.[114] На овај начин, системи ВИ заобилазе забрану која произилази из чл. 17, што захтева нову правну доктрину која би препознала инференцијалне податке као објекат заштите под истим режимом као и изворне посебне врсте података.[115]

2.4. Право на ограничење обраде у примени вештачке интелигенције

Члан 31. ЗЗПЛ омогућава лицу на које се подаци односе да од руковаоца захтева ограничење обраде својих података у специфичним ситуацијама тј. ако оспорава тачност података, ако је обрада незаконита а лице се противи брисању, ако контролору подаци више нису потребни али их лице захтева ради подношења правних захтева, или ако је лице поднело приговор на обраду (сходно члану 37). Током периода ограничења, подаци се могу само чувати, док је свака друга обрада (осим уз пристанак или ради заштите права другог лица/јавног интереса) забрањена.

Право на ограничење обраде представља својеврсну „правну кочницу" која спречава даљу употребу спорних података док се не утврди њихов статус. Етичке смернице дају овом члану посебну димензију кроз сегмент који се односи на деловање и контролу а који инсистира на томе да системи ВИ треба да буду подршка лицима на начин да им омогуће да задрже суштинску контролу над аутоматизованим процесима. Надаље, Етичке смернице кроз начело достојанства истичу да појединац не сме бити подређен функцијама система, што у контексту предметног члана значи да корисник мора имати ефективну аутономију над својим дигиталним идентитетом. Стога, чл. 31 служи као механизам којим се осигурава транспарентност и управљање подацима кроз цео животни циклус система, приморавајући руковаоца да технички онемогући коришћење одређеног сета података унутар сложених алгоритамских операција када корисник активира своје право на контролу.

Примена ВИ трансформише право на ограничење обраде у озбиљан технички изазов будући да када лице на кога се подаци односе захтева да се његови подаци ограниче од стране руковаоца, онда руковаоц мора имати могућност да те податке заиста ограничи на

[114] P. Hacker, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, Common Market Law Review, vol. 55, no. 4, 2018, 1146–1148.
[115] B. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, L. Floridi, *The Ethics of Algorithms: Mapping the Debate*, Big Data & Society, vol. 3, no. 2, 2016, 3.

начин да онемогући њихово коришћење за даљи тренинг или фино подешавање модела. То даље значи успостављање механизама који омогућавају легитимисан приступ и контролу података кроз цео животни циклус система, што приморава програмере да развију модуларне структуре података.[116] Узимајући у обзир склоност одређених модела ВИ да генеришу нетачне информације, чл. 31 постаје примарни алат за заштиту тачности. Лице може захтевати ограничење обраде док руковаоц не верификује изведене закључке, чиме се спречава да нетачне претпоставке постану основа за даље профилисање.[117] Уколико лице поднесе приговор на профилисање, чл. 31 обавезује на привремено заустављање процеса. Ово је директна примена етичког принципа транспарентности и одговорности, којим се спречава да се над појединцем врши неоправдан или нејасан надзор док се не утврди претежни интерес руковаоца.[118]

Интеграцијом чл. 31. ЗЗПЛ и етичких постулата о суверенитету корисника, ограничење обраде података у домену ВИ прераста у кључни инструмент за очување људског достојанства, осигуравајући да појединац у дигиталном поретку остане активан субјект са правом вета на неконтролисану алгоритамску анализу.

2.5. Аутоматизовано доношење појединачних одлука и профилисање у примени вештачке интелигенције

Члан 38. ЗЗПЛ дефинише право да лице на које се подаци односе не буде предмет одлуке донете искључиво на основу аутоматизоване обраде, укључујући и профилисање, ако та одлука производи правне последице по то лице или на сличан начин значајно утиче на његов положај. Законодавац предвиђа изузетке у случајевима неопходности или за извршење уговора између лица на које се подаци односе у руковаоца, заснованости на посебном закону или изричитог пристанка лица (ст. 2). Међутим, чак и када су изузеци примењиви, руковалац је императивно обавезан да спроведе одговарајуће мере заштите права, што

[116] G. Sartor, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, European Parliament, Brussels, 2020, 46–49, преузето 17.01.2026, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.
[117] B. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, L. Floridi, *op. cit*., 6.
[118] L. Edwards, M. Veale*, op. cit*., 34.

примарно обухвата право на људску интервенцију, право на изражавање сопственог става и право на оспоравање одлуке пред овлашћеним лицем (ст. 3).

Предметни члан представља правну брану против „диктатуре алгоритама", а своје суштинско упориште проналази у Етичким смерницама. Етичке смернице дефинишу кључно деловање и надзор на начин да се инсистира на томе да системи ВИ морају бити дизајнирани тако да омогуће људима доношење информисаних одлука и очување основних права. Људски надзор се према Етичким смерницама реализује кроз три техничка модалитета: људска интервенција, који омогућава интервенцију у сваком циклусу одлучивања; људски надзор који се односи на могућност деловања током рада система и људско одлучивање који подразумева контролу над целокупном активношћу и могућност искључења система. Тиме се осигурава да се аутономија појединца не подреди функцијама система. Системи ВИ су инхерентно усмерени ка потпуној аутоматизацији, што чини примену чл. 38 критичном тачком заштите посматрано кроз ефикасност људске интервенције, објашњивост и право на приговор као и заштиту од дискриминације. У контексту ВИ, људска интервенција из чл. 38 не сме бити симболична. Применом принципа људског одлучивања из Етичких смерница, руковаоц је дужан да обезбеди да лице које врши надзор поседује неопходна знања и овлашћења да суштински измени или поништи алгоритамску одлуку, чиме се спречава појава тзв. алгоритамске пристрасности.[119] Да би лице ефикасно оспорило одлуку, оно мора разумети логику обраде. Иако ЗЗПЛ не именује експлицитно право на објашњење, Етичке смернице кроз сегмент транспарентности захтевају објашњивост модела, што је технички предуслов за остваривање права из чл. 38.[120] Став 4 предметног члана забрањује аутоматизовано одлучивање над посебним врстама података (из чл. 17), што је у складу са циљем Етичких смерница који се односи на правичност а у оквиру кога се истиче заштита од неоправдане пристрасности, дискриминације и стигматизације.

Члан 38 ЗЗПЛ, ојачан прецизним механизмима људског надзора из Етичких смерница, представља коначни правни гарант да вештачка интелигенција остаје алат у служби човека, а не аутономан ентитет који доноси неопозиве одлуке о људским судбинама.

[119] L. Edwards, M. Veale, *op. cit*., 36.
[120] G. Sartor, *op. cit*., 55.

2.6. Мере заштите у примени вештачке интелигенције

Члан 42 ЗЗПЛ конституише обавезу руковаоца да имплементира техничке и организационе мере заштите кроз два кључна концепта: интегрисану заштиту и подразумевану заштиту. Према ст. 1, руковаоц је дужан да већ у фази одређивања средстава обраде, као и током саме обраде, примени мере попут псеудонимизације које су дизајниране за ефикасну примену начела заштите података. Став 2 обавезује руковаоца да примени мере које осигуравају да се по аутоматизму обрађују само они подаци који су неопходни за сваку конкретну сврху обраде, што се односи на обим прикупљених података, степен њихове обраде и период чувања.

Предметни члан представља оперативни превод етичких принципа у инжењерске захтеве. Етичке смернице наглашавају да техничка поузданост и безбедност морају бити интегрални део животног циклуса система ВИ. У том смислу, чл. 42 ЗЗПЛ није само законска обавеза, већ методолошки оквир за програмере који захтева да заштита приватности не буде „накнадна памет“, већ конститутивни елемент кода. Такође, Стратегија развоја вештачке интелигенције у Републици Србији за период 2025-2030. године истиче развој софтверских решења која подржавају приватност као кључну компоненту за изградњу поверења друштва у ВИ технологије.

Примена система ВИ доводи до суштинске трансформације тумачења чл. 42, померајући фокус са формалне на интегрисану заштиту. За разлику од традиционалних база података, ВИ захтева технике попут диференцијалне приватности, која омогућава тренинг модела на великим сетовима података без откривања идентитета појединаца.[121] Интегрисана заштита из чл. 42 овде подразумева обавезу руковаоца да изабере оне структуре које по дизајну онемогућавају реинжењеринг података о личности из готовог модела. С обзиром на то да системи ВИ имају тежњу ка масовном прикупљању података ради веће прецизности, принцип подразумеване заштите из ст. 2 долази у директан сукоб са техничком потребом за

[121] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, L. Zhang, *Deep Learning with Differential Privacy*, 2016, 2, преузето 14.01.2026, https://www.researchgate.net/publication/386862898_Deep_Learning_with_Differential_Privacy.

додатним подацима. Законска обавеза је да систем, у свом основном подешавању, прикупља минимум података, што код ВИ захтева строгу селекцију само релевантних карактеристика већ у претходној фази процесуирања.[122] Интегрисана заштита обухвата и заштиту модела од напада као што је тзв. инверзија модела тј. покушај нападача да реконструише оригиналне податке из модела. Етичке смернице изричито захтевају креирање отпорности на такве нападе, што подиже праг пажње из чл. 42 на ниво који захтева континуирано тестирање модела ВИ на слабе стране пре њиховог пуштања у рад.

Имплементација чл. 42 ЗЗПЛ у развоју ВИ захтева суштинску промену парадигме заштите са правне дедукције на техничку индукуцију где заштита података престаје да буде спољни захтев и постаје инжењерски стандард без којег систем ВИ не може бити сматран законитим нити поузданим.

2.7. Безбедност обраде у примени вештачке интелигенције

Члан 50 ЗЗПЛ налаже руковаоцу и обрађивачу обавезу примене одговарајућих техничких, организационих и кадровских мера како би се обезбедио ниво безбедности који одговара ризику. Став 1 овог члана прецизира да те мере, између осталог, обухватају псеудонимизацију и криптовање, способност обезбеђивања трајне поверљивости, интегритета, доступности и отпорности система, као и успостављање процеса редовног тестирања и процењивања делотворности мера безбедности.

Овај члан представља својеврсни технички „штит" заштите података. Етичке смернице под насловом „Техничка поузданост и безбедност" директно се надовезују на чл. 50, истичући да систем ВИ мора бити отпоран на нападе и да мора поседовати планове за ванредне ситуације. Етичке смернице наглашавају да безбедност није једнократни чин, већ континуирани процес надзора. Ово је комплементарно са Стратегијом развоја вештачке интелигенције у Републици Србији 2025-2030 која као један од циљева наводи изградњу безбедног дигиталног окружења за развој иновација.

[122] European Data Protection Board (EDPB), *Guidelines 04/2019 on Article 25 Data Protection by Design and by Default*, *op. cit.*, 15.

Безбедност из чл. 50 у контексту ВИ подразумева заштиту од напада где нападач уноси суптилне промене у податке како би преварио алгоритам. То рецимо може бити и промена само неколико пиксела на слици која ВИ може навести на погрешну дијагнозу. С тим у вези сматрамо да је руковалац дужан да примени мере које ове нападе чине неуспешним, поред своје законске обавезе заједно са обрађивачем да свако лице које има овлашћени приступ подацима о личности исте податке обрађује искључиво по налогу руковаоца или ако је на то обавезно законом (ст. 5). Мере безбедности морају обухватити спречавање контаминације података где се у базу за учење подмећу компромитовани подаци како би се искривили будући резултати рада ВИ.[123] Члан 50. налаже руковаоцу да обезбеди интегритет комплетног ланца података.

Сходно наведеном, чл. 50 ЗЗПЛ у симбиози са етичким захтевима за поузданошћу система ВИ прераста оквире класичне заштите сервера, постајући императив за очување функционалног и етичког интегритета ВИ у свим фазама њеног животног циклуса.

2.8. Процена утицаја на заштиту података о личности у примени вештачке интелигенције

Члан 54 ЗЗПЛ прописује обавезу руковаоца да изврши процену утицаја предвиђених радњи обраде на заштиту података о личности пре него што са обрадом отпочне. Ова обавеза настаје када је вероватно да ће врста обраде, посебно уз коришћење нових технологија и узимајући у обзир њену природу, обим, околности и сврху, проузроковати висок ризик по права и слободе физичких лица. Став 3 посебно истиче да је процена неопходна код систематске и свеобухватне процене личних својстава лица која се заснива на аутоматизованој обради (профилисање) и код обраде посебних врста података (чл. 17) у великом обиму.

[123] European Data Protection Board (EDPB), *Guidelines 01/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications*, 22–23, преузето 20.01.2026, https://www.edpb.europa.eu/system/files/202103/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf.

Овај члан представља алат за управљање ризицима. Етичке смернице наглашавају неопходност процене утицаја на основна права као део одговорности и транспарентности. Смернице сугеришу да процена утицаја не сме бити само папиролошка формалност, већ суштински процес који идентификује потенцијалне пристрасности алгоритма и негативне друштвене ефекте. Такође, Стратегија развоја вештачке интелигенције у Републици Србији 2025- 2030. године види ову процену као механизам за изградњу поверења грађана у државне и приватне сервисе ВИ.

Сагледавањем предметног члана кроз термине као што су „нове технологије“ и „висок ризик“ могли бисмо рећи да примена ВИ по дефиницији активира обавезе о процени утицаја. Већина система ВИ врши профилисање које води ка одлукама из чл. 38, што према Поверенику за информације од јавног значаја представља радњу за коју је процена утицаја на заштиту података о личности обавезна.[124] Руковалац мора детаљно описати структуру алгоритма и оправдати неопходност такве обраде. У оквиру чл. 54, руковалац је дужан да процени ризик од неправедних исхода по различите групе лица. Ово захтева тестирање модела на репрезентативним подацима како би се спречило да ВИ дискриминише на основу заштићених карактеристика.[125]

Сходно наведеном, чл 54. ЗЗПЛ представља најзначајнију процедуралну брану којом се спречава неодговорна имплементација ВИ, приморавајући руковаоце да правне и етичке последице алгоритамског одлучивања сагледају пре него што систем произведе непоправљиве последице по појединца.

2.9. Претходно мишљење Повереника у примени вештачке интелигенције

Члан 55. ЗЗПЛ успоставља обавезу руковаоца да се обрати Поверенику за информације од јавног значаја и заштиту података о личности ради прибављања мишљења пре отпочињања обраде, уколико извршена процена утицаја из чл. 54 укаже да би планирана

[124] Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника за информације од јавног значаја и заштиту података о личности, бр. 021-00-14/2019-4 од 19.06.2019. године, *Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности*, преузето 12.02.2026, https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/zastitapodataka/Odlukaprocenauticaja.pdf.
[125] F. J. Zuiderveen Borgesius, *op. cit.*, 24.

обрада проузроковала висок ризик по права и слободе лица, а руковалац није у могућности да тај ризик ублажи прихватљивим мерама заштите. Повереник је дужан да у року од 60 дана , а који се може продужити за још 45 дана, достави писмено мишљење руковаоцу, а уколико сматра да би планирана обрада била у супротности са законом, може искористити своја овлашћења за забрану обраде.

Овај члан представља врхунац принципа одговорности у дигиталном поретку. Етичке смернице наглашавају важност надзора и одговорности, сугеришући да се за системе ВИ који задиру у основна људска права мора обезбедити екстерни ниво контроле. У том смислу, чл. 55 ЗЗПЛ делује као регулаторни сигурносни вентил који спречава пуштање у рад алгоритама чији су ризици (нпр. системска дискриминација или угрожавање приватности великих размера) остали нерешени на нивоу самог руковаоца.

Специфичност ВИ често доводи до „неотклоњивих ризика“ тако да примена чл. 55 постаје неизбежна приликом примене ВИ. Када руковалац у оквиру процене утицаја утврди да због природе тзв. црне кутије не може у потпуности да предвиди понашање модела ВИ у свим граничним случајевима, настаје обавеза консултације са Повереником према чл. 55. Ово је кључно за осигурање транспарентности коју захтевају и Етичке смернице. С обзиром на то да је биометријски надзор на јавним местима класификован као операција изузетно високог ризика, Повереник је у својој досадашњој пракси истицао да је претходно мишљење из чл. 55 обавезно за овакве системе ВИ како би се спречио незаконит масовни надзор.

Сходно наведеном, чл. 55 ЗЗПЛ представља коначну институционалну кочницу у процесу имплементације ВИ, која кроз обавезни дијалог између иноватора и Повереника гарантује да технолошки напредак неће бити остварен на штету основних слобода и правне сигурности грађана Републике Србије.

ЗАКЉУЧАК

Спровођењем обухватне правне анализе заштите података о личности у контексту примене вештачке интелигенције, долазимо до фундаменталног закључка да се налазимо на прекретници правне цивилизације. ВИ више није само футуристички концепт или напредна грана рачунарства, већ „активни супстрат“ који суштински мења природу приватности и аутономију појединца. Кроз развој од реактивних машина до сложених система са ограниченом меморијом и теоријских концепата самосвести, ова технологија је показала да поседује моћ редефинисања основних људских права. Основни налази овог рада указују на то да је традиционални концепт заштите података, заснован на статичној обради, постао недовољан пред динамичном и често непредвидивом природом машинског учења.

Кључни резултат истраживања огледа се у идентификацији онтолошког сукоба између техничке потребе алгоритама за експанзивношћу и правног императива за минимизацијом. ВИ своју прецизност црпи из корелација које су често невидљиве људском разуму, док право инсистира на јасно дефинисаној сврси и ограничењу обраде. Овај сукоб је најочигледнији у домену тзв. инференцијалних података. На основу спроведене анализе, закључујемо да системи ВИ могу са застрашујућом тачношћу извести закључке о посебним категоријама података попут здравственог стања, политичких уверења или сексуалне оријентације користећи наизглед потпуно неутралне параметре. Овај феномен *de facto* заобилази строге забране из члана 17. ЗЗПЛ и ГДПР, стварајући правни вакуум који захтева нову доктрину према којој изведени подаци морају уживати исти степен заштите као и изворно прикупљени осетљиви подаци.

У погледу међународног и европског правног оквира, закључујемо да је Европска унија направила историјски искорак усвајањем Акта о ВИ. Овај пропис не дерогира ГДПР, већ му даје неопходну техничку оперативност. Наша анализа показује да је Акт о ВИ коначно решио дугогодишњу доктринарну дебату о праву на објашњење. Док је у оквиру ГДПР ово право често остајало у сенци рецитала и пословне тајне, Акт о ВИ га поставља као

императив за системе високог ризика. Тиме је транспарентност трансформисана из правне декларације у инжењерски захтев. Кључни налаз у овом сегменту је да без објашњивости алгоритама, право на приговор и право на оспоравање одлуке остају само „мртво слово на папиру“.

Посебна пажња у закључним разматрањима мора се посветити правном систему Републике Србије. Србија је, кроз ЗЗПЛ из 2018. године, успешно хармонизовала своје законодавство са европским стандардима, али примена тих норми на системе ВИ открива специфичне изазове. Анализа члана 38. ЗЗПЛ, који регулише аутоматизовано доношење појединачних одлука и профилисање, показује да је то „последња линија одбране“ људског достојанства. Налази рада указују на то да људска интервенција не сме бити симболична или про форма. Да би заштита била ефикасна, човек који надзире систем мора поседовати суштинску моћ и техничко разумевање да поништи алгоритамску одлуку. У супротном, суочавамо се са опасностима алгоритамске пристрасности која може институционализовати дискриминацију под плаштом објективне технологије.

Истраживање је потврдило и критичну важност Процене утицаја на заштиту података из члана 54. ЗЗПЛ. У контексту ВИ, ова процена престаје да буде административни терет и постаје примарни алат за управљање ризицима. Закључујемо да је за већину система ВИ израда ове процене законски обавезна због високог ризика и употребе нових технологија. Такође, улога Повереника за информације од јавног значаја као институционалног коректива из члана 55. ЗЗПЛ је незаменљива. Претходно мишљење Повереника мора бити обавезна степеница за сваки систем масовног биометријског надзора, јер такви системи директно угрожавају анонимност грађана у јавном простору, што представља неприхватљив ризик у демократском друштву.

На етичком плану, симбиоза права и Етичких смерница за поуздану ВИ коју смо анализирали, показује да будућност заштите података лежи у интеграцији права и технологије. Концепти интегрисане и подразумеване заштите (члан 42. ЗЗПЛ) морају постати део образовног програма не само правника већ и инжењера. Заштита приватности мора бити уткана у сваки слој неуронске мреже, а не накнадно додата као законска исправка. Само кроз такав приступ можемо обезбедити да ВИ остане „алат“, а не „господар“ друштвених процеса.

У завршници свакако можемо рећи да вештачка интелигенција није правно несавладива, али захтева активан и проактиван надзор. Домаћи правни систем поседује јако добру основу, али пракса великих технолошких компанија у Србији указује на потребу за већом одлучношћу у примени санкција када се крше начела транспарентности и правичности. Основно људско право на заштиту података о личности у дигиталном поретку не сме бити предмет трговине за ефикасност алгоритама. Право мора остати врховни арбитар који гарантује да ће свака одлука која значајно утиче на човека бити донета на начин који је разуман, поштен и, изнад свега, подложан људском суду. Овај рад је скроман допринос разумевању те сложене симбиозе, са надом да ће будућа законска решења још јаче штитити оно што је у дигиталној ери најлакше изгубити а то је наша приватност и наша суштинска људска слобода.

ЛИТЕРАТУРА

1. Агенција Европске уније за основна права и Савет Европе, *Приручник о европском праву заштите података*, Агенција Европске уније за основна права и Савет Европе, Луксембург, 2018, преузето 11.01.2026, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_sr.pdf.
2. С. Андоновић, Д. Прља, *Основи права заштите података о личности*, Институт за упоредно право, Београд, 2020.
3. M. Abadi, A. Chu, I. Goodfellow, B. McMahan, I. Mironov, K. Talwar, L. Zhang, *Deep Learning with Differential Privacy*, 2016, 1–11, преузето 14.1.2026, https://www.researchgate.net/publication/386862898_Deep_Learning_with_Differential_Privacy ,
4. F. Z. Zuiderveen Borgesius, *Discrimination, Artificial Intelligence and Algorithmic Decision-Making*, Council of Europe, Strasbourg, 2018.
5. L. A. Bygrave, *Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decision-Making*, in: M. Ienca, O. Pollicino, L. Liguori, E. Stefanini, R. Andorno (eds.), *Information Technology, Life Sciences and Human Rights*, Cambridge University Press, Cambridge, 2022, 166-188.
6. L. A. Bygrave, *Information Law: From the Incunabula of Privacy to the Eras of Big Data and Artificial Intelligence*, Oxford University Press, Oxford, 2014.
7. M. Ebers, *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in: L. DiMatteo, C. Poncibo, M. Cannarsa (eds.), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, Cambridge, 2021, 321-344.
8. L. Edwards, M. Veale, *Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For*, Duke Law & Technology Review, vol. 16, no. 1, 2017, 18-84.
9. L. Floridi, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford University Press, Oxford, 2019.
10. С. Гајин, *Заштита података о личности у сектору безбедности: водич кроз законску регулативу*, Центар за унапређивање правних студија; Организација за европску безбедност и сарадњу, Мисија ОЕБС-а у Србији, Београд, 2019.
11. Д. Гајић, *Заштита података о личности према Уставу СРЈ и предлогу закона о заштити података о личности*, Гласник Адвокатске коморе Војводине, вол. 68, бр. 9, 1996, 346-359.
12. M. Furmankiewicz, A. Sołtysik-Piorunkiewicz, P. Ziuziański, *Artificial Intelligence and Multi-Agent Software for E-Health Knowledge Management System*, Informatyka Ekonomiczna, vol. 32, no. 2, 2014, 51-63.
13. P. Hacker, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law*, Common Market Law Review, vol. 55, no. 4, 2018, 1143-1185.
14. M. Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Cheltenham, 2015.

15. K. Yeung, *Why Worry About Decision-Making by Machine?*, in: K. Yeung, M. Lodge (eds.), *Algorithmic Regulation*, Oxford University Press, Oxford, 2019, 21-49.
16. B. J. Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice*, Scripted, vol. 8, no. 3, 2011, 229-256.
17. A. M. Kristen, J. Ugander, *Monophily in Social Networks Introduces Similarity among Friends-of-Friends*, Nature Human Behaviour, vol. 2, no. 4, 2018, 284-290.
18. C. Kuner, L. Bygrave, K. Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020.
19. М. Кузминац, *Заштита података о личности: питање будућности које је „предухитрила" садашњост*, Правни записи, вол. XV, бр. 2, 2024, стр. 562-577.
20. J. McCarthy, M. Minsky, N. Rochester, C. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, AI Magazine, vol. 27, no. 4, 2006, 12-14.
21. Merriam-Webster Dictionary, *artificial intelligence*, преузето 10.12.2025, https://www.merriam-webster.com/dictionary/artificial%20intelligence.
22. М. Милосављевић, *Вештачка интелигенција*, Универзитет Сингидунум, Београд, 2015.
23. B. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, L. Floridi, *The Ethics of Algorithms: Mapping the Debate*, Big Data & Society, vol. 3, no. 2, 2016, 1-26.
24. Д. Прља, Г. Гасми, В. Корађ, *Вештачка интелигенција у правном систему ЕУ*, Институт за упоредно право, Београд, 2021.
25. Radu, R. *Negotiating Internet Governance*, Oxford University Press, Oxford, 2019,
26. G. Sartor, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, European Parliament, Brussels, 2020, преузето 17.01.2026. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf
27. J. Searle, *Minds, Brains, and Programs*, Behavioral and Brain Sciences, vol. 3, no. 3, 1980, 417-424.
28. M. Scherer, *Artificial Intelligence and Legal Decision-Making: The Wide Open?*, Journal of International Arbitration, vol. 36, no. 5, 2019, 540-573.
29. В. Спасић, *Утицај вештачке интелигенције на ауторско право*, у: Н. Раичевић (ур.), *Одговорност у правном и друштвеном контексту*, Тематски зборник радова Правног факултета у Нишу, Ниш, 2023, 105–131.
30. Share фондација, *Мета променила политику приватности: Наши подаци као материјал за тренинг АИ*, преузето 11.01.2026, https://sharefoundation.info/meta-promenila-politiku-privatnosti-nasi-podaci-kao-materijal-za-trening-ai/.
31. H. Sroka, W. Wolny, *Inteligentne systemy wspomagania decyzji*, Wydawnictwo AE, Katowice, 2009.
32. A. Turing, *Computing Machinery and Intelligence*, Mind, vol. 59, no. 236, 1950, 433-460.
33. S. Wachter, *The Theory of Artificial Immutability: Protecting Algorithmic Groups under Anti-Discrimination Law*, Tulane Law Review, vol. 97, no. 2, 2023, 1-50.
34. S. Wachter, B. Mittelstadt, *A Right to Reasonable Algorithmic Decision-Making: Unpacking Data Protection Law's Untapped Potential*, Columbia Business Law Review, 2019, 497-619.
35. S. Wachter, B. Mittelstadt, C. Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, Harvard Journal of Law & Technology, vol. 31, no. 2, 2018, 842-887.

36. S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, International Data Privacy Law, vol. 7, no. 2, 2017, 1-24.
37. M. Wooldridge, *A Brief History of Artificial Intelligence: What It Is, Where We Are, Where We Are Going*, Flatiron Books, Great Britain, 2021.
38. E. Wolfgang, *Grundkurs Künstliche Intelligenz: eine praxisorientierte Einführung*, Institut für Künstliche Intelligenz, Weingarten, 2016.
39. M. Vitajić, *Ethical and Practical Challenges of Artificial Intelligence (AI) in Legal Practice and Judiciary*, in: M. Matić Bošković, J. Kostić (eds.), *Shaping Justice: How Penal Law and Judiciary Address Contemporary Societal Challenges*, Institute of Comparative Law; Institute of Criminological and Sociological Research; Judicial Academy, Belgrade, 2025, 107-121.
40. M. Veale, F. J. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, Computer Law Review International, vol. 22, no. 4, 2021, 97-112.
41. F. J. Zuiderveen Borgesius, Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence, The International Journal of Human Rights, vol. 24, no. 10, 2020, 1572-1593.

Коришћена документација

1. *Annex III: High-Risk AI Systems Referred to in Article 6(2)*, преузето 01.12.2025, https://artificialintelligenceact.eu/annex/3/.
2. *Binding Decision 2/2023 on the Dispute Submitted by the Irish SA regarding TikTok Technology Limited*, The Data Protection Commission, 1.9.2023, преузето 10.01.2026, https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en.
3. *Case of Malone v. the United Kingdom (Application no. 8691/79), 2 August 1984,* преузето 3.2.2026, *https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57533%22]}*.
4. *Charter of Fundamental Rights of the European Union* (2000/C 364/01), преузето 5.2.2026, https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
5. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data*, преузето 5.2.2026, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
6. *Етичке смернице за развој, примену и употребу поуздане и одговорне вештачке интелигенције*, Службени гласник РС, бр. 23/2023.
7. European Commission for the Efficiency of Justice (CEPEJ), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment*, Council of Europe, 2018, преузето 17.12.2025, https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf.
8. European Data Protection Board (EDPB), *Report of the Work Undertaken by the ChatGPT Taskforce*, преузето 30.01.2026, https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf.

9. European Data Protection Board (EDPB), *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, преузето 11.1.2026, https://www.edpb.europa.eu/system/files/2022-05/edpb_guidelines_202205_frtlawenforcement_en_1.pdf.
10. European Data Protection Board (EDPB), *Guidelines 08/2020 on the Protection of Personal Data in the Context of the Use of AI*, преузето 4.12.2025, https://www.edpb.europa.eu/system/files/202104/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.
11. European Data Protection Board (EDPB), *Guidelines 01/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications*, преузето 20.1.2026, https://www.edpb.europa.eu/system/files/202103/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf.
12. European Data Protection Board (EDPB), *Guidelines 04/2019 on Article 25 Data Protection by Design and by Default*, преузето 10.11.2025, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
13. *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251rev.01, adopted on 3 October 2017, 19-21, преузето 07.12.2025.
14. *Одлука о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника за информације од јавног значаја и заштиту података о личности*, бр. 021-00-14/2019-4 од 19.06.2019. године, преузето 12.2.2026, https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/zastitapodataka/Odlukaprocenauticaja.pdf.
15. Предмет бр. 072-04-296/2021-07 од 26.2.2021. године, *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, публикација бр. 7, Београд, 2022.
16. Предмет бр. 073-14-2819/2021-02 од 2.11.2021. године, *Заштита података о личности: Ставови и мишљења Повереника за информације од јавног значаја и заштиту података о личности*, публикација бр. 7, Београд, 2022.
17. *Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, преузето 5.2.2026, https://rm.coe.int/16808ac918.
18. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, преузето 29.11.2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
19. *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)*, преузето 03.12.2025, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

20. *Стратегија развоја вештачке интелигенције у Републици Србији за период 2025–2030. године*, Службени гласник РС.
21. *Resolution adopted by the General Assembly on 18 December 2013, 68/167: The Right to Privacy in the Digital Age*, преузето 4.2.2026, https://documents.un.org/doc/undoc/gen/n13/449/47/pdf/n1344947.pdf.
22. *Revised Draft Resolution on the Right to Privacy in the Digital Age*, A/C.3/71/L.39, преузето 4.2.2026, https://digitallibrary.un.org/record/848969?ln=en&v=pdf.
23. *Universal Declaration of Human Rights*, 1948, преузето 29.12.2025, https://www.un.org/en/about-us/universaldeclaration-of-human-rights.
24. *Закон о електронским комуникацијама*, Службени гласник РС, бр. 44/2010, 60/2013 – одлука УС, 62/2014, 95/2018 – др. закон и 35/2023 – др. закон.
25. *Закон о информационој безбедности*, Службени гласник РС, бр. 91/2025.
26. *Закон о матичним књигама*, Службени гласник РС, бр. 20/2009, 145/2014 и 47/2018.
27. *Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података*, Службени лист СРЈ – Међународни уговори, бр. 1/92.
28. *Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода измењене у складу са Протоколом број 11, Протокола уз Конвенцију за заштиту људских права и основних слобода, Протокола број 4 уз Конвенцију за заштиту људских права и основних слобода којим се обезбеђују извесна права и слободе који нису укључени у Конвенцију и Први протокол уз њу, Протокола број 6 уз Конвенцију за заштиту људских права и основних слобода о укидању смртне казне, Протокола број 7 уз Конвенцију за заштиту људских права и основних слобода, Протокола број 12 уз Конвенцију за заштиту људских права и основних слобода и Протокола број 13 уз Конвенцију за заштиту људских права и основних слобода о укидању смртне казне у свим околностима*, Службени лист СЦГ – Међународни уговори, бр. 9/2003, 5/2005, 7/2007 – испр., и Службени гласник РС – Међународни уговори, бр. 12/2010 и 10/2015.
29. *Устав Републике Србије*, Службени гласник РС, бр. 98/2006 и 115/2021.
30. *Устав Савезне Републике Југославије*, Службени лист СРЈ, бр. 1/92.
31. *Закон о раду*, Службени гласник РС, бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 – одлука УС, 113/2017, 95/2018 – аутентично тумачење и 109/2025 – др. закон.
32. *Закон о ратификацији међународног пакта о грађанским и политичким правима*, Службени лист СФРЈ, бр. 7/71.
33. *Закон о слободном приступу информацијама од јавног значаја*, Службени гласник РС, бр. 120/2004, 54/2007, 104/2009, 36/2010 и 105/2021.
34. *Закон о заштити података о личности*, Службени гласник РС, бр. 87/2018.
35. *Закон о заштити података о личности*, Службени гласник РС, бр. 97/2008, 104/2009 – други закон, 68/2012 – одлука УС РС и 107/2012.
36. *Закон о заштити података о личности*, Службени лист СРЈ, бр. 24/98.
37. *Закон о здравственој документацији и евиденцијама у области здравства*, Службени гласник РС, бр. 92/2023.

Интернет извори

1. Legitimni interes kao pravni osnov za obradu podataka o ličnosti - Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti.

САЖЕТАК

Примена вештачке интелигенције суштински мења природу заштите приватности, трансформишући личне податке из пасивних записа у активне параметре за доношење аутоматизованих одлука. Основна напетост коју овај рад анализира лежи у сукобу између технолошке експанзивности алгоритама и правне рестриктивности норми у вези са заштитом података. Док системи машинског учења црпе своју прецизност из масовне експлоатације података, правни поредак, кроз Општу уредбу о заштити података и домаћи Закон о заштити података о личности, инсистира на начелу минимизације и јасно дефинисаној сврси. Овај сукоб престаје да буде само теоријски у тренутку када системи тзв. црне кутије почну да генеришу. инференцијалне податке. Реч је о способности вештачке интелигенције да из наизглед неутралних дигиталних трагова изведе закључке о најосетљивијим аспектима личности као што је здравствено стање, политичко уверење или сексуална оријентација чиме се *de facto* заобилазе строге законске забране обраде посебних категорија података.

Кључни механизам заштите пронађен је у концепту објашњивости и операционализацији транспарентности. Нови регулаторни оквир, предвођен Актом о вештачкој интелигенцији, пребацује терет са права појединца да тражи објашњење на обавезу програмера да системе учине транспарентним по самом дизајну. Посебан фокус истраживања стављен је на на људску интервенцију код аутоматизованог одлучивања. Надзор од стране човека не сме бити само формалан, већ суштински, са стварном моћи оспоравања алгоритамских исхода који производе правне последице по појединца.

У домаћем правном контексту, рад идентификује Процену утицаја на заштиту података као примарну процедуралну брану којом се спречава неодговорна имплементација високих технологија. Институционална улога Повереника, кроз механизам претходног мишљења, појављује се као неопходан сигурносни вентил код система изузетно високог ризика, попут неселективног биометријског надзора који угрожава анонимност у јавном простору. Вештачка интелигенција мора остати алат у служби човека, а заштита података конститутивни елемент сваког кода. Само кроз симбиозу правних норми и техничких стандарда може се осигурати да економски интерес развоја алгоритама не потисне

фундаментално право на људско достојанство и информационо самоопредељење у дигиталном добу.

Кључне речи: вештачка интелигенција, заштита података о личности, Закон о заштити података о личности, Општа уредба о заштити података, Акт о вештачкој интелигеницји

SUMMARY - Protection of Personal Data in the Domain of Artificial Intelligence

The application of artificial intelligence fundamentally reshapes the nature of privacy protection, transforming personal data from passive records into active inputs for automated decision-making. The central tension examined in this paper arises from the interplay between the technological expansiveness of algorithmic systems and the normative constraints imposed by data protection law. While machine learning systems derive their accuracy from the large-scale processing of data, the legal framework, most notably the General Data Protection Regulation and the Serbian Law on Personal Data Protection insists upon the principles of data minimisation and purpose limitation. This tension ceases to be merely theoretical once so-called "black-box" systems begin to generate inferential data. In this context, artificial intelligence is capable of deriving conclusions about highly sensitive aspects of an individual's identity - such as health status, political beliefs, or sexual orientation from seemingly neutral digital traces, thereby effectively circumventing the strict legal prohibitions governing the processing of special categories of personal data.

A key protective mechanism is identified in the concept of explainability and the implementation of transparency principles. The emerging regulatory framework, led by the Artificial Intelligence Act, shifts the focus from the individual's right to obtain an explanation to the obligation of system designers and developers to ensure transparency by design. Particular emphasis is placed on human intervention in automated decision-making processes. Human oversight must not remain merely formal, but must be substantive, with a genuine capacity to challenge and override algorithmic outcomes that produce legal or similarly significant effects for individuals.

Within the domestic legal context, the paper identifies the Data Protection Impact Assessment as the primary procedural safeguard against the irresponsible deployment of advanced technologies. The institutional role of the Commissioner, exercised through the mechanism of prior opinion, emerges as an essential safety valve in the context of high-risk systems, such as indiscriminate biometric surveillance, which can undermine anonymity in public spaces. Artificial intelligence must remain a tool in the service of humanity, with data protection embedded as a

constitutive element of system design. Only through a coherent alignment of legal norms and technical standards can it be ensured that the economic imperatives driving algorithmic innovation do not prevail over the fundamental right to human dignity and informational self-determination in the digital age.

Keywords: artificial intelligence, personal data protection, Serbian Law on Personal Data Protection, General Data Protection Regulation, Artificial Intelligence Act

БИОГРАФИЈА

Александра Миљковић је рођена 05.11.1993. године, у Нишу, Републици Србији. Завршила је основну школу „Душан Радовић“ у Нишу, а након тога је завршила Правно пословну школу у Нишу. После завршене средње школе, 2012. године је уписала Правни факултет за привреду и правосуђе у Новом Саду, који је завршила у року, дана 02.02.2017. године, са просечном оценом 7,19.

Приправнички стаж је обавила у адвокатској канцеларији у Нишу, код адвоката Ненада Крстића, у периоду од 11.04.2017. до 11.04.2021. године. У том периоду је обављала послове адвокатског приправника, састављала тужбе, предлоге, молбе, правне лекове и друге поднеске, као и заступала правна и физичка лица, нарочито у грађанским и привредним споровима. Положила је правосудни испит у Београду, дана 15.07.2020. године.

Дана 01.05.2021. године постаје корисник почетне обуке на Правосудној академији у Београду, где је прошла кроз: Кривично одељење Вишег суда у Београду, у већу судије Оливере Ђурић; Прво основно јавно тужилаштво у Београду - Одељење за насиље у породици, где јој је ментор била заменик јавног тужиоца Гордана Радић; Прекршајно одељење Прекршајног суда у Београду, у већу судије Миријане Ашковић; Парнично одељење Другог основног суда у Београду, у већу судије Милице Горавице; Парнично одељење Вишег суда у Београду, у већу судије Мирјане Илић-Михаиловић, где и данас наставља своју обуку, усавршавајући се у изради судских одлука и руковођењу судским поступком.

Завршила је програм почетне обуке и успешно положила завршни испит на Правосудној академији у Београду 04.10.2023. године, са завршном оценом 5. Током обуке учествовала је на бројним панел дискусијама, предавањима и семинарима, укључујући: „Антидискриминационо право“ (2021), „Дискриминација у области рада и запошљавања“ (2021), „Еколошко право“ (2021), „Образлагање судских одлука и људска права“ (2022), „Образлагање судских одлука и људска права – пракса Уставног суда“ (2022), „Одузимање имовине проистекле из кривичног дела“ (2022), „Имовинска права и Европска конвенција о људским правима“ (2023), „Породични закон – специјализација из области права детета“ (2023), „Сексуално насиље-изазови у доказивању и разумевању положаја жртве“ (2024), „Редефинисање концепта јурисдикције у дигитално доба“ (2024), „Обука из медијације“ (2024).

Уписала је мастер студије 2024. године, на Правном факултету Универзитета у Нишу - смер право и информационе технологије, са циљем да додатно унапреди своје правно знање.

У слободно време бави се сликарством. Говори енглески језик.

АЛЕКСАНДРА МИЉКОВИЋ

Е-маил: aleksandramiljkovic0511@gmail.com

ИЗЈАВА О ИСТОВЕТНОСТИ

ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА

Име и презиме аутора мастер рада: _____

Наслов мастер рада:_____

_____

Ментор: _____

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

У Нишу, _____

Потпис аутора

_____

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом _____

_____

пријављен и одбрањен на Правном факултету Универзитета у Нишу:

• резултат сопственог истраживачког рада;

• да овај мастер рад у целини, нити у деловима, нисам пријављивао/ла на другим факултетима, нити универзитетима;

• да нисам повредио/ла ауторска права, нити злоупотребио/ла интелектуалну својину других лица.

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

Аутор мастер рада: _____

У Нишу, _____

Потпис аутора

_____