

УНИВЕРЗИТЕТ У НИШУ
ПРАВНИ ФАКУЛТЕТ

**Права лица чији се подаци о личности обрађују
од стране модела вештачке интелигенције**

(мастер рад)

Коментори:
Проф. др Дејан Вучетић
др Велимир Илић

Студент:
Ленка Секулић
Број индекса: M013/24-ИТ

Ниш, 2026.

САДРЖАЈ

УВОД	1
I ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ	4
1. Појам вештачке интелигенције	4
2. Улога података у вештачкој интелигенцији	5
3. Заштита података о личности у вештачкој интелигенцији	6
II СУБЈЕКТИ УКЉУЧЕНИ У ОБРАДУ ПОДАТАКА ОД СТРАНЕ МОДЕЛА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ	11
1. Појам и обим одговорности руковоаца	11
2. Појам и обим одговорности обрађивача	12
3. Субјекти предвиђени Уредбом ЕУ о вештачкој интелигенцији и обим њихове одговорности	13
4. Обавезе у вези са начином остваривања права	14
III ПРАВО НА ИНФОРМИСАНОСТ И ПРАВА У ВЕЗИ СА АУТОМАТИЗОВАНИМ ДОНОШЕЊЕМ ОДЛУКА	16
1. Право лица да буде информисано о обради	16
1.1. Пружање информација лицу када су подаци прикупљени директно од њега	17
1.2. Пружање информација лицу када подаци нису прикупљени директно од њега	18
1.3. Додатно информисање о обради од стране модела вештачке интелигенције	19
1.4. Нејасноће у законским одредбама	20
1.5. Изузеци од обавезе непосредног информисања лица о обради	22
1.6. Начин пружања информација	24
2. Аутоматизовано доношење одлука и профилисање	26
3. Проблем објашњивости модела вештачке интелигенције	29
IV ПРАВО НА ПРИСТУП И ПРЕНОСИВОСТ ПОДАТАКА	32
1. Право на приступ	32
2. Право на преносивост података о личности	35
V ПРАВО НА ИСПРАВКУ И БРИСАЊЕ ПОДАТАКА	37
1. Право на исправку и допуну	37
2. Право на брисање	39
VI ПРАВО НА ОГРАНИЧЕЊЕ ОБРАДЕ И ПРИГОВОР	44

1.	Право на ограничење обраде	44
2.	Право на приговор	45
VII ДАЉИ РАЗВОЈ ПРАВА ЛИЦА ЧИЈИ СЕ ПОДАЦИ О ЛИЧНОСТИ ОБРАЂУЈУ ОД СТРАНЕ МОДЕЛА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ		48
	ЗАКЉУЧАК	51
	ПОПИС КОРИШЋЕНЕ ЛИТЕРАТУРЕ	54
	ПОПИС ОСТАЛЕ ИСТРАЖИВАЧКЕ ГРАЋЕ	58
	САЖЕТАК	60
	ABSTRACT	62
	БИОГРАФИЈА СТУДЕНТА	64

УВОД

Некада је било незамисливо да ће технологија која уме да предузима самосталне мисаоне операције и радње постати незаобилазан део сваког разговора. Компаније у разним индустријама се такмиче у томе ко ће пре аутоматизовати што више својих операција, нуде се курсеви о томе како користити моделе вештачке интелигенције, а већина платформа и апликација које свакодневно користимо садрже функције које се заснивају на технологији вештачке интелигенције.

Вештачка интелигенција се користи у различитим гранама индустрије и за различите задатке. На пример, у рад машина у фабрикама је често укључен неки вид ове технологије како би могле самостално да извршавају задатке. Међутим, они системи који су тренутно у жижи јавности у вези са законским уређењем њиховог рада су модели које појединци непосредно користе и којима су подаци о личности неопходни за функционисање. Између осталог, ту спадају системи који врше функцију агента, четботови, генеративна вештачка интелигенција, системи који се користе за алгоритме на друштвеним мрежама и системи који анализирају податке.

Европска унија је у почетку развоја заштите података о личности била у несумњивој предности у регулисању ове материје, али данас већина држава света има своје законе који постављају одређене стандарде заштите података о личности. Међутим, тренутно важећа легислатива је махом усвојена пре него што је технологија напредовала у протеклих неколико година. Законодавци широм света покушавају да одрже корак са брзим развојем технологије којом се обрађују подаци о личности. Тражи се приступ којим се не би гушиле иновације и развој тржишта, али би се истовремено на адекватан начин заштитила права појединаца. Неминовно је да ће се технологија даље мењати, али је тешко предвидети са сигурношћу које ће се све иновације јавити и када. Стога је важно да законодавство буде што више технолошки неутрално, што подразумева да садржи правила која нису везана за одређену технологију или начин обраде података.

Специфичности технологије вештачке интелигенције доводе до дилеме око тога у којој мери су постојећа правила технолошки неутрална и применљива на обраду коју врши модел вештачке интелигенције. Овај рад се усредсређује на разматрање те дилеме када су у питању права лица на која се подаци односе у вези са обрадом. Суштина признавања ових права појединцима је да им се додели моћ да одлучују и контролишу

шта ће се дешавати са њиховим подацима.¹ Она омогућавају очување слободе и суверености појединаца у ери у којој су подаци о личности један од највреднијих добара. Међутим, права могу испунити своју улогу и бити делотворна само ако је појединац свестан да их има и ако му је пружена ефективна могућност да их оствари, што се може довести у питање у случају вештачке интелигенције.

Посматрајући досадашњу праксу већине компанија које се јављају у улози руковалаца и добављача система вештачке интелигенције, чини се да се усаглашавају са законом само онолико колико морају. Надзорна тела за заштиту података о личности држава чланица Европске уније покушавају да заштите појединце изрицањем мера овим компанијама, као и покретањем судских поступака, што резултује високим казнама. Међутим, чак ни високе казне нису довољне да промене приоритете компанија које често зарађују много више од казне коју су дужне да плате. Ни чињеница да се модел развија у оквиру Европске уније не значи да ће се модел потпуно усклађивати са законом. На пример, Mistral, руковалац са седиштем у Европској унији, објављује документацију о усклађености са прописима,² али су истраживања показала да и даље има низак ниво транспарентности.³

Овај рад ће најпре изложити појам вештачке интелигенције, улогу података у њеном раду и законски оквир заштите података о личности у Републици Србији и Европској унији у виду осврта на изворе права и надзорна тела. Рад ће се уз то бавити и питањем одређивања обима обавеза руковалаца, обрађивача и субјеката дефинисаних Уредбом Европске уније о вештачкој интелигенцији у вези са остваривањем права лица на која се подаци односе. Уследиће излагање права, што обухвата право на информисаност о обради, права лица у вези са аутоматизованим доношењем одлука и профилисањем, право на приступ подацима, право на преносивост података, право на исправку и допуну, право на брисање, право на ограничење обраде и право на приговор. Рад ће размотрити њихов садржај, изузетке од обавезе остваривања права, као и могућност и модалитете њиховог остваривања када обраду врши модел вештачке интелигенције. На крају ће бити размотрен даљи развој законодавства у Републици Србији и Европској унији који је од

¹ J. Castellanos Claramunt, La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos, *Métodos de Información*, Vol. 11(21), p. 61.

² Mistral, *AI Governance*; преузето 07.10.2026. <https://legal.mistral.ai/>

³ Stanford Institute for Human Centered Artificial Intelligence, Center for Research on Foundation Models – CRFM, *The 2025 Foundation Model Transparency Index*; преузето 12.08.2026. <https://crfm.stanford.edu/fmti/December-2025/paper.pdf>

значаја за права лица на која се подаци односе у контексту вештачке интелигенције. Циљ ће бити идентификовати потенцијалне правне празнине у тренутном законском оквиру којим се регулише ова материја, као и установити постојећа и могућа законска и технолошка решења којима би се отклониле сметње у остваривању права. Рад се бави обрадом података о личности од стране модела вештачке интелигенције када су руковаоци приватна лица, те не разматра обраду коју врше надлежни органи у посебне сврхе и одредбе закона применљиве на њу.

Методологија која је коришћена при писању рада обухвата нормативни, догматски и упоредни метод, као и метод анализе садржаја и анализе случаја. Истраживање је спроведено анализом и тумачењем закона, мишљења надлежних тела и стручњака за предметну област, као и постојеће праксе тамо где је она релевантна за проблематику рада. Излагање налаза истраживања може приближити појединцима права која имају и начин на који вештачка интелигенција обрађује њихове податке о личности, али и бити од користи руковоцима за боље разумевање садржаја и могућности остваривања њихових обавеза.

I ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА И ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ

Убрзани развој технологије довео је до развоја различитих области вештачке интелигенције које су ушле у свакодневну употребу. Оне се заснивају на напредним алгоритмима за обучавање, а као „гориво“ за рад алгоритми користе велику количину података. Систем може користити визуелне улазне податке за закључивање, као што то чини рачунарски вид (*computer vision*). Такође, у стању је да податке из природног говора или текста преведе на језик разумљив машини, обради их и поново преведе на природни језик, што је задатак обраде природних језика (*natural language processing – NLP*). Поред тога, развија се и роботика у оквиру које системи могу да разумеју и обрађују улазне податке из више различитих сензора, дају излазни податак у виду повратне информације, али и да као резултат закључивања предузму одговарајуће радње у физичком свету. У употреби су и експертски системи, који се на специфичном скупу података тренирају тако да поседују специјализована знања и умеју да извршавају компликоване задатке у одређеној области, као што је медицина.

1. Појам вештачке интелигенције

Разумевање појма вештачке интелигенције није једноставан задатак, узимајући у обзир све различите форме у којима се јавља ова технологија. Њен детаљан опис може бити у потпуности јасан само стручњацима. Међутим, када закон регулише неку технологију, потребно је да она буде прецизно дефинисана како не би било сумње у вези са тим на шта се примењују постављена правила. Законодавци то чине тако што истичу особине на основу којих се технологија може сврстати у одређену категорију. Самим тим, појам „вештачке интелигенције“ обухвата различите врсте технологије које поседују особине постављене дефиницијом.

Независна експертска група Европске комисије за вештачку интелигенцију (*The European Commission's High-Level Expert Group on Artificial Intelligence*; у даљем тексту: AI HLEG) у својој дефиницији вештачке интелигенције истиче следеће особине:

- у питању је систем који је дизајнирао човек;
- систем предузима радње у физичком или дигиталном свету;
- радње се могу састојати из опажања сопственог окружења, тумачења података, логичког размишљања, закључивања коришћењем знања које је систем стекао на основу података, као и одлучивања коју ће наредну радњу да предузме;
- радње се извршавају како би се остварио сложен циљ који је постављен систему;

- систем може бити пројектован да анализира како његове радње утичу на његово окружење и да тако научи да прилагођава своје понашање.⁴

Уредба ЕУ о вештачкој интелигенцији⁵ је преузела неке од елемената дефиниције коју је дао AI HLEG. Уредба дефинише систем вештачке интелигенције (*AI system*) као машински систем пројектован да ради на различитим нивоима аутономије, а који након увођења може да покаже прилагодљивост. Поред тога, такав систем је у стању да закључи како да генерише излазне из улазних вредности како би остварио експлицитне или имплицитне циљеве. Према Уредби, излазне вредности се могу јавити у виду предвиђања, садржаја, препоруке или одлуке који могу утицати на физичка или дигитална окружења.⁶

Уредба не дефинише општи појам „модела вештачке интелигенције“, али га сматра за део система вештачке интелигенције, који сачињава уз додатне компоненте, попут корисничког интерфејса.⁷ За потребе овог рада, појам „модел вештачке интелигенције“ користиће се као општи појам за технологију вештачке интелигенције која је способна да обрађује податке о личности и која се на њима учи.⁸

2. Улога података у вештачкој интелигенцији

Могућности модела и квалитет његове способности закључивања засновани су на квалитету података који се користе за учење. „Учење“ и „тренирање“ система се у овом раду користе као синоними за процес чији је циљ да модел може самостално да закључује на основу скупа података које је користио за учење. Ово је принцип који се пре свега примењује у машинском учењу. Једна од грана машинског учења је дубоко учење, у оквиру ког се овај процес спроводи путем мреже која је пројектована налик мрежи људских неурона.⁹ Везе између „неурона“ се подешавају у складу са напретком учења

⁴ The European Commission's High-Level Expert Group on Artificial Intelligence, *A Definition of AI: Main Capabilities and Scientific Disciplines*; преузето 23.09.2026.

https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

⁵ 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) (у даљем тексту: EU AI Act)

⁶ Art. 3(1) EU AI Act.

⁷ Recital 97 EU AI Act.

⁸ European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*; преузето 04.10.2026.

https://www.edpb.europa.eu/system/files/documents/2024-12/edpb_opinion_202428_ai-models_en.pdf

⁹ Д. Прља, Г. Гасми, В. Кораћ, *Вештачка интелигенција у правном систему ЕУ*, Београд, 2021, стр. 67.

система. Крајњи излазни податак биће онај за који систем процени да има највише вероватноће да буде тачан у конкретној ситуацији на основу датих улазних података.

Подаци за учење могу бити означени, као у случају надзираног учења (*supervised learning*). На пример, код класификације, тренинг подаци се обележавају према својој припадности некој од одређених група, како би модел из њих извукао карактеристике на основу којих се класификују у ту групу. Са друге стране, ненадзирано учење (*unsupervised learning*) подразумева да модел нема означене податке већ сам уочава сличности и разлике између њих, на основу чега их затим сврстава у одвојене категорије. Учење је успешно ако модел може да уочи обрасце у новим подацима које је приметио у тренинг подацима и да „разуме“ којој групи би припадао тај нови податак. Једна од врста учења је и појачано учење (*reinforcement learning*), приликом кога подаци нису означени, али модел добија позитивну или негативну повратну информацију на основу које учи какве радње треба извршити.¹⁰

Поред учења, постоје различити процеси у систему вештачке интелигенције који користе податке. Систем путем сензора добија улазне податке, које преводи у формат који може да разуме и обради. На основу тих података, систем доноси закључке, планира, претражује базе података, проналази најбоље решење и одлучује коју радњу треба предузети. Своје закључке систем може да преведе назад у језик разумљив човеку и да их пружи као излазне податке, а може и самостално предузимати одговарајуће радње.¹¹

Процес учења и рада модела није савршен и може доћи до грешака у излазним подацима. Када модел као излазни податак пружи нетачне информације, такве грешке се називају „халуцинације“.¹² Модел их може поткрепити нетачно наведеним изворима, због чега оне делују као тачне и проверене информације.

3. Заштита података о личности у вештачкој интелигенцији

Сви процеси вештачке интелигенције у којима се користе подаци могу укључивати податке о личности, у зависности од састава скупа података за учење као и улазних података које систем прикупља. Ради давања одговора на питања од значаја за заштиту података о личности, потребно је најпре разумети законски оквир у коме ће се она

¹⁰ *ibid.*, стр. 71.

¹¹ The European Commission's High-Level Expert Group on Artificial Intelligence, *op. cit.*

¹² B. Fernández Delgado, V. Cazurro Barahona, Can artificial intelligence forget? Reflections on the right to disappear in a world where algorithms remember everything, *International Journal of Engineering Business Management*, Vol. 18, p. 6.

разматрати. Република Србија усвојила је 2018. године Закон о заштити података о личности (у даљем тексту: ЗЗПЛ).¹³ Надлежни орган који има задатак да надзире његову примену је Повереник за информације од јавног значаја и заштиту података о личности. Повереник је у свом досадашњем раду објавио приручнике који садрже карактеристичне поступке у којима је одлучивао. Његова пракса може бити користан извор који руковалац и обрађивач могу консултовати када Закон није прецизно уредио неки појам. Тренутно се ради на усвајању новог закона, те ће овај рад размотрити и одређене предложене одредбе у Нацрту закона о заштити података о личности које су релевантне за права лица на која се подаци односе.¹⁴

Државе чланице Европске уније су најпре, на начин који је њима највише одговарао, уводиле у своје прописе о заштити података о личности одредбе Директиве 95/46/ЕЗ.¹⁵ Тако је настао проблем неуједначеног регулисања ове материје међу различитим државама чланицама, на који је Европска унија одговорила усвајањем Опште уредбе о заштити података о личности (у даљем тексту: GDPR).¹⁶ GDPR омогућава непосредну и уједначену применљивост свих правила о заштити података о личности широм Европске уније.

Свака држава чланица је одредила независно надзорно тело (*supervisory authority*) које спроводи надзор над применом GDPR-а. Ови органи решавају по притужбама појединаца и усвајају препоруке и упутства о разним аспектима заштите података о личности. Ставови које заузимају у овим документима, као и када доносе одлуке у оквиру својих надлежности, могу бити користан извор тумачења GDPR-а.

Важна тумачења даје и Европски одбор за заштиту података (*European Data Protection Board*, у даљем тексту: EDPB). Овај орган састављен је од представника надзорних тела сваке државе чланице и Европског надзорника за заштиту података (*European Data Protection Supervisor*, у даљем тексту: EDPS), те његови ставови представљају консензус свих ових органа. До сада је EDPB усвојио значајан број водича којима се тумаче разна питања у оквиру заштите података о личности, а између осталог и примена одредби

¹³ Закон о заштити података о личности, *Службени гласник РС*, бр. 87/2018-54.

¹⁴ Министарство правде, *Нацрт закона о заштити података о личности*; преузето 11.08.2026.
<https://mpravde.gov.rs/javne-rasprave>

¹⁵ 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.

¹⁶ 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).

GDPR-a на обраду коју врше нове технологије. Поред тога, и сам EDPS усваја водиче о заштити података о личности.

Европском одбору за заштиту података претходила је Радна група из члана 29.¹⁷ У питању је било саветодавно тело које је такође усвојило мишљења и водиче о разним питањима заштите података о личности. Многе водиче Радне групе је EDPB званично одобрио, те се такође могу користити као извор тумачења GDPR-a.

ЗЗПЛ и GDPR су у великој мери подударни прописи. Због тога се у овом раду законске одредбе излажу на начин на који су формулисане ЗЗПЛ-ом, уз истовремено упућивање на комплементарне одредбе GDPR-a и истицање евентуалних уочених разлика.

Како би се неки податак сматрао податком о личности, потребно је да садржи карактеристике предвиђене законским дефиницијама овог појма. Податак о личности се у ЗЗПЛ-у и GDPR-у дефинише на сличан начин, као „сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета“.¹⁸ Ова дефиниција се може разложити на више појединачних карактеристика:

- то може бити сваки податак који садржи наведене карактеристике,
- податак се односи на одређено лице,
- потребно је да то буде физичко лице, и
- идентитет лица на које се податак односи је непосредно или посредно одређен или одредив.¹⁹

Податак не мора да буде непосредно о појединцу како би се сматрало да се односи на њега. Податак о личности може бити и информација која се превасходно односи на нешто друго, али која ће се вероватно користити у сврхе евалуације или другачијег третмана појединца, или може имати утицаја на његова права.²⁰

¹⁷ Агенција Европске уније за основна права и Савет Европе, *Приручник о европском праву заштите података*; преузето 11.08.2026. <https://poverenik.rs/h-content/uploads/2024/03/HF42-prirucnik-evropsko-pravo-zastite-podataka-SRP-poverenik.pdf>

¹⁸ Чл. 4. т. 1. ЗЗПЛ; Art. 4 (1) GDPR. (члан 4. став 1. тачка 1))

¹⁹ Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*; преузето 29.09.2026. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

²⁰ European Data Protection Board, *Guidelines 02/2026 on Anonymisation*; преузето 29.09.2026. https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en

Ако идентитет лица није одређен на основу конкретног податка, биће одредив ако је доступан неки додатан податак који ће омогућити његову идентификацију. Самим тим, важно је установити коме је тај податак доступан, јер ће тај субјекат онда моћи да одреди идентитет лица.²¹ Ово је потребно оценити у сваком појединачном случају и у односу на сваког субјекта који учествује у обради података. Приликом процене узимају се у обзир сва средства за која је „разумно вероватно“ да ће их тај субјекат искористити за идентификацију.²² „Разумна вероватноћа“ се може проценити на основу потребних средстава и времена, технологије која је у датом тренутку доступна том субјекту, као и њеног даљег развоја.²³ Поред тога, разматрају се и фактори попут врсте и карактеристика података, могућности приступа подацима, контекста њиховог обрађивања, али и постојања и доступности додатних информација које би допринеле идентификацији лица.²⁴

Уколико се податак не односи на неко физичко лице, или ако оно није одређено или одредиво на основу податка, податак се може сматрати анонимизованим за конкретног субјекта. Ово је релевантно из разлога што се прописи заштите података о личности не примењују на анонимизоване податке.²⁵

Скупови података које користи и на којима се учи модел вештачке интелигенције углавном садрже и податке о личности и анонимизоване податке. Потребно је у том смислу осврнути се на ситуацију у којој скуп података истовремено садржи и посебне врсте података о личности, и податке који не спадају у ту категорију. Када скуп података садржи макар један податак који спада у посебне врсте података о личности, ограничења применљива на посебне врсте података о личности примениће се на целокупан скуп података уколико се ти подаци не могу одвојити.²⁶ Аналогно, скуп података који садржи и анонимизоване податке и податке о личности сматраће се као скуп података о личности уколико се ти подаци не могу одвојити или се скуп посматра и третира као целина.²⁷

Модел вештачке интелигенције који је користио податке о личности у процесу учења не чува те податке у њиховом изворном облику након учења. Из њих извлачи

²¹ Case C-413/23 P, *European Data Protection Supervisor (EDPS) v Single Resolution Board (SRB)*, para. 84.

²² Recital 26 GDPR.

²³ *ibid.*

²⁴ European Data Protection Board, *Guidelines 02/2026 on Anonymisation*, *op. cit.*

²⁵ Recital 26 GDPR.

²⁶ Case C-252/21, *Meta v Bundeskartellamt*, para. 89.

²⁷ European Data Protection Board, *Guidelines 02/2026 on Anonymisation*, *op. cit.*

статистичке обрасце које касније примењује у закључивању, те се заправо утицај података чува у моделу уместо самог податка. Међутим, истраживања су показала да је модел у стању да касније генерише фрагменте тих података или закључке које је донео на основу њих, као и да искористи научене статистичке обрасце како би генерисао конкретан податак о личности на коме се учио.²⁸ Како би се сматрало да је модел „анонимизован“ иако је користио податке о личности за учење, потребно је да могућност да се ти подаци извуку из модела буде занемарљива.²⁹

На крају, важна карактеристика модела вештачке интелигенције је да неминовно води ка стварању „изведених података“ (*inferred data*). У питању су подаци попут закључака, предвиђања и претпоставки које модел створи на основу других података. Подаци на основу којих је модел створио изведене податке не морају нужно бити подаци о личности да би се и изведени подаци сматрали подацима о личности,³⁰ већ ће се тако окарактерисати на основу тога да ли испуњавају услове предвиђене дефиницијом података о личности.³¹ Проблематика о којој се том приликом може говорити везана је за могућност остваривања права појединаца у односу на такве податке.

²⁸ B. Fernández Delgado, V. Cazurro Barahona, *op. cit.*, p. 3.

²⁹ European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, *op. cit.*

³⁰ European Data Protection Board, *Guidelines 02/2026 on Anonymisation*, *op. cit.*

³¹ Case C-434/16, *Peter Nowak v Data Protection Commissioner*, paras. 42–44.

II СУБЈЕКТИ УКЉУЧЕНИ У ОБРАДУ ПОДАТАКА ОД СТРАНЕ МОДЕЛА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ

Поступак обраде коју врши модел вештачке интелигенције може бити сложен и укључивати више субјеката. Самим тим, пре излагања садржаја права која лица имају у вези са својим подацима о личности, важно је разумети врсте субјеката предвиђене законом који ће бити одговорни за њихово остваривање. Ово поглавље објашњава појмове руковоаца и обрађивача, као и субјекте које предвиђа Уредба ЕУ о вештачкој интелигенцији и идентификује обим њихове одговорности. Поред тога, разматрају се опште обавезе у вези са начином на који је потребно одговорити на захтеве лица и обезбедити остваривање права.

1. Појам и обим одговорности руковоаца

Појам руковоаца развио се како би било могуће одредити субјекта који ће сносити највећу одговорност за законитост обраде података о личности. Ово произилази из тога што је у питању правно или физичко лице које одређује у које сврхе и на који начин ће се подаци обрађивати,³² што значи да се обрада одвија примарно у његовом интересу. Није нужно да руковалац непосредно учествује у обради података о личности како би био одговоран за то да сви услови постављени законом буду испуњени. Руковалац се одређује у сваком конкретном случају на основу околности које су присутне, али може бити одређен и законом којим се прописује обрада података о личности. Тада закон одређује сврху и начин обраде уместо неког субјекта, али му истовремено и приписује одговорност за закониту обраду.³³

Многобројне обавезе руковоаца имају за циљ да се обезбеди адекватна заштита лица на која се подаци односе. Руковалац мора да усвоји одговарајуће техничке, организационе и кадровске мере како би обрада била у складу са законом, узимајући у обзир њену природу, обим, околности и сврху, као и вероватноћу наступања ризика по појединце и његов ниво. Такође, треба да поседује одговарајуће интерне правне акте којима се обезбеђује усклађеност обраде са законом,³⁴ као и да буде у могућности да је докаже.³⁵ У контексту предмета овог рада, руковалац је субјекат према коме појединци остварују своја права и који је одговоран за испуњење њихових захтева.

³² Чл. 4. т. 8. ЗЗПЈ; Art. 4 (7) GDPR.

³³ *ibid.*

³⁴ Чл. 41. ст. 3. ЗЗПЈ; Art. 24 (2) GDPR.

³⁵ Чл. 41. ст. 1. ЗЗПЈ; Art. 24 (1) GDPR.

Може се десити да више субјеката истовремено одлучује како ће се и зашто обрађивати подаци о личности. Тада се говори о „заједничким руковаоцима“. Они имају обавезу да уреде међусобне односе како би било јасно ко ће бити одговоран за испуњење обавеза прописаних законом. Различити заједнички руковаоци могу бити одговорни за различите обавезе. Између осталог, важно је одредити ко ће бити одговоран да испуни захтеве за остваривање права лица у вези са обрадом.³⁶ Независно од тога како су заједнички руковаоци међусобно уредили своју одговорност, појединац свакако може остваривати своја права у односу на било кога од њих.³⁷

2. Појам и обим одговорности обрађивача

Руковалац може сам да врши обраду података, а може и да целокупну обраду или један њен део повери субјекту који се назива обрађивач. Овај субјекат обрађује податке о личности искључиво у име и на основу упутстава руковаоца. Једно исто лице може истовремено бити руковалац за неке радње обраде, а обрађивач за друге. Дакле, улога се процењује за сваку појединачну радњу обраде.³⁸ Радње обраде се међусобно разликују на основу засебне сврхе и правног основа. Такође, обрађивач може постати руковалац када изврши радњу обраде независно од упутстава првобитног руковаоца, уз одређене изузетке у којима је обавезан да обрађује податке.³⁹ Разликовање обрађивача и руковаоца је важно јер обрађивач има мање одговорности и обавеза у односу на руковаоца, у складу са тиме што не одређује како ће се подаци обрађивати.

С обзиром на то да је одговорност за закониту обраду на руковаоцу, он има и обавезу да повери обраду само оним обрађивачима који пружају гаранције да примењују адекватне техничке, организационе и кадровске мере, као и да обраду врше на начин који омогућава усклађеност са законом, укључујући и заштиту лица на која се подаци односе.⁴⁰ Однос између руковаоца и обрађивача мора бити уређен уговором или другим правно обавезујућим актом. Њиме се, између осталог, обрађивач обавезује да, у мери у којој је то могуће узимајући у обзир природу обраде, примени одговарајуће техничке, организационе и кадровске мере којима би помогао руковаоцу да испуни своје обавезе у

³⁶ Чл. 43. ст. 2–4. ЗЗПЈ; Art. 26 (1), (2) GDPR.

³⁷ Чл. 43. ст. 7. ЗЗПЈ; Art. 26 (3) GDPR.

³⁸ European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*; преузето 26.09.2026. https://www.edpb.europa.eu/documents/guideline/guidelines-072020-on-the-concepts-of-controller-and-processor-in-the-gdpr_en

³⁹ *ibid.*

⁴⁰ Чл. 45. ст. 1. ЗЗПЈ; Art. 28 (1) GDPR.

вези са захтевима лица за остваривање њихових права.⁴¹ Дакле, обим одговорности обрађивача зависиће од конкретних околности радњи обраде, као и правног акта који уређује његов однос са руковоцем, а којим се може прецизирати које обавезе обрађивач има у овом смислу. Некад се то може свести само на прослеђивање руковоцу захтева који обрађивач добије, а у другим случајевима обрађивач може бити у обавези да предузме одређене техничке мере којима се омогућава остваривање права појединаца.⁴²

3. Субјекти предвиђени Уредбом ЕУ о вештачкој интелигенцији и обим њихове одговорности

Развој и употреба система вештачке интелигенције често укључује субјекте чија је улога и могућност да утичу на усклађеност модела са законом различита и зависи од стадијума развоја модела. Од тога полази и Уредба ЕУ о вештачкој интелигенцији када предвиђа више различитих субјеката и сваком од њих одређује обим одговорности. С обзиром на сложен сплет субјеката и њихових улога током животног века модела, од велике је важности да између њих постоји сарадња како би се омогућило остваривање права појединаца у вези са обрадом.⁴³ Важно је напоменути да се многе од предвиђених обавеза односе на високоризичне системе вештачке интелигенције.

На почетку животног века система, „добављач“ (*provider*) је субјекат који развија модел, те је на њему примарна одговорност у фази тренирања високоризичног модела. „Субјекат који уводи систем“ (*deployer*) прибавља систем који је добављач претходно ставио у промет и употребљава га у оквиру своје надлежности. Самим тим, субјекат који уводи систем је одговоран за усклађеност са законом у фази коришћења модела. У контексту права лица на која се подаци односе, субјекат који уводи систем је према Уредби одговоран да осигура испуњење права и да појединцима пружи информације о систему и њиховим правима.⁴⁴ Са друге стране, добављач високоризичних система мора да развије систем на начин на који ће субјекту који га уводи бити јасно како систем функционише и која су његова ограничења, као и да му пружи те информације у виду инструкција.⁴⁵ Тако се омогућава субјекту који уводи систем да испуњава обавезе транспарентности и информисања лица о одлукама које високоризични систем доноси,

⁴¹ Чл. 45. ст. 4. т. 5. ЗЗПЈ; Art. 28 (3)(e) GDPR.

⁴² European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, *op. cit.*

⁴³ B. Fernández Delgado, V. Cazurro Barahona, *op. cit.*, p. 6.

⁴⁴ Recital 93 EU AI Act.

⁴⁵ Art. 13 EU AI Act.

као и логици иза тих одлука, уколико то објашњење није већ предвиђено и пружено на основу одредби GDPR-а.⁴⁶

Поред тога, добављач је одговоран да високоризични систем развије на начин који омогућава људски надзор над његовим функционисањем,⁴⁷ чиме би се између осталог омогућило учешће човека у преиспитивању одлука донетих аутоматизованом обрадом података. Субјекат који уводи систем ће потом бити одговоран да омогући појединцу да остварује своја права у вези са одлуком.

Одређивање руковаоца међу субјектима дефинисаним Уредбом ЕУ о вештачкој интелигенцији зависиће од тога ко одлучује о начину и сврси обраде података о личности. Може се десити да се сваки субјекат у једном тренутку нађе у улози руковаоца. Добављач би се, на пример, сматрао руковоцем у фази тренирања модела у оном обиму у коме одлучује о сврхама и начинима обраде тренинг података. Са друге стране, субјекат који уводи систем ће углавном одлучивати о сврхама и начинима обраде података о личности приликом каснијег коришћења модела, те ће тада бити истовремено и руковалац у односу на обраду података о личности.

Закључак је да се улоге морају процењивати у сваком конкретном случају у односу на одређену радњу обраде, узимајући у обзир критеријуме постављене и Уредбом и GDPR-ом. Ова два прописа су независна један од другог, али треба имати у виду да Уредба у неким деловима упућује на обавезе прописане GDPR-ом и приписује одговорност за њихово испуњење одређеном субјекту, попут субјекта који уводи систем.⁴⁸

4. Обавезе у вези са начином остваривања права

Руковалац је дужан да помогне и обезбеди могућност појединцу да оствари своја права,⁴⁹ укључујући и могућност да захтев за остваривање права поднесе електронским путем, нарочито када се на тај начин обрађују подаци о личности.⁵⁰ Поступак остваривања права не сме да траје дуго. Када прими захтев, руковалац је дужан да лице обавести о поступању по његовом захтеву без одлагања, а најкасније у року од 30 дана од дана пријема захтева. Рок може бити продужен за још 60 дана ако је то неопходно у складу са сложеношћу и бројем захтева које је руковалац примио, о чему је дужан да

⁴⁶ Art. 86 & Recital 171 EU AI Act.

⁴⁷ Art. 14(1) EU AI Act.

⁴⁸ Art. 26(9) EU AI Act.

⁴⁹ Чл. 21. ст. 2. ЗЗПЈ; Art. 12(2) GDPR.

⁵⁰ Recital 59 GDPR.

обавести појединца.⁵¹ У случају обраде на коју је применљив GDPR, овај рок износи месец дана, а може бити продужен за још два месеца.⁵²

Одређена права подложна су ограничењима, али је потребно ограничења применити рестриктивно и процењивати оправданост позивања на њих у сваком конкретном случају. Када руковалац не поступи по захтеву лица из било ког разлога, потребно је да га о тим разлозима, као и праву да се обрати Поверенику или суду, обавести без одлагања, а најкасније 30 дана од дана пријема захтева,⁵³ односно месец дана у случају обраде на коју је применљив GDPR.⁵⁴

Начелно, руковалац не наплаћује накнаду за поступање по захтеву за остваривање права. Међутим, он има право да наплати нужне административне трошкове поступања по захтеву уколико је захтев „очигледно неоснован или претеран, а посебно ако се исти захтев учестало понавља“.⁵⁵ Уместо наплате трошкова, руковалац може у том случају и да одабере да не поступи по захтеву.⁵⁶ Свакако, терет доказивања оваквог карактера захтева је на руковаоцу.⁵⁷

Изложена правила применљива су на остваривање свих права, али је потребно да се сагледају и особености сваког појединачног права јер су могућности њиховог остваривања у случају обраде коју врши модел вештачке интелигенције различите.

⁵¹ Чл. 21. ст. 3. ЗЗПЈ.

⁵² Art. 12(3) GDPR.

⁵³ Чл. 21. ст. 4. ЗЗПЈ.

⁵⁴ Art. 12(4) GDPR.

⁵⁵ Чл. 21. ст. 5. т. 1. ЗЗПЈ; Art. 12(5)(a) GDPR.

⁵⁶ Чл. 21. ст. 5. т. 2. ЗЗПЈ; Art. 12(5)(b) GDPR.

⁵⁷ Чл. 21. ст. 6. ЗЗПЈ; Art. 12(5) GDPR.

III ПРАВО НА ИНФОРМИСАНOST И ПРАВА У ВЕЗИ СА АУТОМАТИЗОВАНИМ ДОНОШЕЊЕМ ОДЛУКА

Право лица да буде информисано о обради укључује и право да буде информисано о постојању и детаљима аутоматизованог доношења одлука, те су у овом поглављу након анализе општег права на информисаност изложена и остала права која лице има у вези са таквом обрадом. Поред тога, ово поглавље идентификује и проблем објашњивости модела вештачке интелигенције који може отежати остваривање ових права.

1. Право лица да буде информисано о обради

Информисаност о обради података је један од основних услова који омогућава појединцима да остварују своја права. Уколико неко не зна да се његови подаци о личности обрађују, нити која права има у вези са својим подацима, неће ни покушавати да их остварује иако би можда желео да заштити своје податке.

Ако се узму у обзир компаније које развијају такозване „основне“ моделе вештачке интелигенције (*foundation AI models*), истраживање спроведено при Универзитету Стенфорд показало је да је њихов ниво транспарентности у 2025. години био прилично низак. Просечан резултат на скали од 100 коришћеној у истраживању био је 40,69. Занимљив закључак је да компаније које своје моделе примарно развијају за друге компаније као клијенте имају виши ниво транспарентности од оних које за кориснике својих модела имају претежно потрошаче. Највећи ниво транспарентности примећен је код компаније IBM, са резултатом 95 од 100, док су још само две компаније имале резултат већи од 50: Writer са 72 и AI21 Labs са 66. Anthropic, Google, Amazon, OpenAI, DeepSeek, Meta и Qwen су оствариле резултат између 26 и 46 од 100, док су најниже рангиране биле Mistral са 18, као и Midjourney и xAI (сада SpaceXAI) са само 14 од 100.⁵⁸ Запажено је да су компаније најмање транспарентне о фази тренирања модела и коришћењу података за тренинг. Као разлог се наводе заштита конкуренције и интелектуалне својине, као и сигурносни ризици.⁵⁹

Законодавство које регулише материју заштите података о личности још увек не садржи специфичне обавезе информисања које би биле применљиве на све случајеве обраде коју врши модел вештачке интелигенције.⁶⁰ Постојеће правне празнине се донекле

⁵⁸ Stanford Institute for Human Centered Artificial Intelligence, Center for Research on Foundation Models – CRFM, *op. cit.*

⁵⁹ *ibid.*

⁶⁰ 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(2), p. 93.

попуњавају додатним обавезама транспарентности које уводи легислатива о вештачкој интелигенцији.

1.1. Пружање информација лицу када су подаци прикупљени директно од њега

Пре свега, потребно је да појединац зна кога и како може да контактира у вези са обрадом. Руковалац мора да идентификује себе, а уз то и да му пружи своје и контакт податке свог представника ако га има, као и лица за заштиту података о личности ако га је именовао.⁶¹

Затим, лице мора бити упознато са сврхом и правним основом обраде.⁶² У случају када је правни основ за обраду легитимни интерес руковоаца, он мора бити назначен.⁶³ Постоје и ситуације у којима је лице дужно да да своје податке руковоацу, ако то захтева закон или уговор. Важно је да зна за постојање те обавезе, као и евентуалних последица уколико одлучи да ускрати давање својих података.⁶⁴ Оваквим информацијама лицу се омогућава да установи да ли је обрада у складу са законом и да је оспорава уколико сматра да није. Ако руковалац намерава да податке даље користи за сврху различиту од оне за коју су првобитно прикупљени, потребно је да о томе обавести појединца, као и да пружи све прописане информације и о тој другој сврси.⁶⁵

Појединац би требало да буде упућен и у то са киме се деле његови подаци, како би могао своја права да остварује и према примаоцима података.⁶⁶ За њега је најправичније да руковалац назначи специфичне примаоце података, али уместо тога може бити обавештен и само о категоријама субјеката којима примаоци припадају.⁶⁷ Радна група из члана 29. наглашава да то укључује информације о активностима које прималац обавља, грани индустрије којој припада, као и његовој локацији.⁶⁸ Потребно је назначити и да се подаци преносе у другу државу или међународну организацију ако је то случај, као и

⁶¹ Чл. 23. ст. 1. т. 1. и 2. ЗЗПЈ; Art. 13(1)(a), (b) GDPR.

⁶² Чл. 23. ст. 1. т. 3. ЗЗПЈ; Art. 13(1)(c) GDPR.

⁶³ Чл. 23. ст. 1. т. 4. ЗЗПЈ; Art. 13(1)(d) GDPR.

⁶⁴ Чл. 23. ст. 2. т. 5. ЗЗПЈ; Art. 13(2)(e) GDPR.

⁶⁵ Чл. 23. ст. 3. ЗЗПЈ; Art. 13(3) GDPR.

⁶⁶ „Прималац” је физичко или правно лице, односно орган власти коме су подаци о личности откривени, без обзира да ли се ради о трећој страни или не, осим ако се ради о органима власти који у складу са законом примају податке о личности у оквиру истраживања одређеног случаја и обрађују ове податке у складу са правилима о заштити података о личности која се односе на сврху обраде (Чл. 4. т. 10. ЗЗПЈ.)

⁶⁷ Чл. 23. ст. 1. т. 5. ЗЗПЈ; Art. 13(1)(e) GDPR.

⁶⁸ Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679*; преузето 16.08.2026. https://www.edpb.europa.eu/documents/guideline/article-29-working-party-guidelines-on-transparency-under-regulation-2016679_en

дати информације о преносу попут тога којим механизмима се обезбеђује да он буде законит.⁶⁹

Од руковаоца се тражи и да назначи колико ће дуго чувати податке. Некад то није могуће прецизно одредити унапред, већ зависи од одређених критеријума, који онда морају да буду назначени.⁷⁰ Поред тога, лице је потребно упутити на права која има у вези са обрадом, као и на њихова евентуална ограничења.⁷¹ Тиме се обезбеђује да су она доступна и лицу које до тада није било информисано о својим правима. Ако лице сматра да обрада података није у складу са законом, може се обратити притужбом Поверенику, те је потребно и то право истакнути у обавештењу о обради.⁷² Када је на обраду применљив GDPR, у питању је право обраћања одговарајућем надзорном телу.⁷³ Уколико постоје заједнички руковаоци, потребно је да суштина њиховог споразума буде доступна лицу, у смислу односа руковалаца са њим и тога које лице је задужено за комуникацију са појединцима на које се подаци односе.⁷⁴

Када обрада подразумева аутоматизовано доношење одлука и профилисање у вези са њим, о чему ће бити реч у наставку рада, важно је да појединац буде адекватно обавештен о томе. Пре свега, руковалац мора да назначи да се одлуке доносе на такав начин, као и да пружи сврсисходне информације о логици која се користи, значају и очекиваним последицама такве обраде.⁷⁵

1.2. Пружање информација лицу када подаци нису прикупљени директно од њега

Руковалац има обавезу да пружи горенаведене информације о обради без обзира на то да ли је податке прикупио директно од лица на које се они односе.⁷⁶ Ипак, постоји разлика у врсти информација које се морају пружити. Ако подаци нису прикупљени директно од лица на које се односе, мора се назначити извор из кога су прикупљени, као и то да је у питању јавно доступан извор ако је то случај. Поред тога, потребно је набројати категорије података које се обрађују. Занимљиво је да се Нацртом закона о заштити података о личности предлаже одредба којом би руковалац био дужан да

⁶⁹ Чл. 23. ст. 1. т. 6. ЗЗПЈ; Art. 13(1)(f) GDPR.

⁷⁰ Чл. 23. ст. 2. т. 1. ЗЗПЈ; Art. 13(2)(a) GDPR.

⁷¹ Чл. 23. ст. 2. т. 2. и 3. ЗЗПЈ; Art. 13(2)(b), (c) GDPR.

⁷² Чл. 23. ст. 2. т. 4. ЗЗПЈ.

⁷³ Art. 13(2)(d) GDPR.

⁷⁴ Чл. 43. ст. 4. ЗЗПЈ; Art. 26(2) GDPR.

⁷⁵ Чл. 23. ст. 2. т. 6. ЗЗПЈ; Art. 13(2)(f) GDPR.

⁷⁶ Чл. 24. ЗЗПЈ; Art. 14 GDPR.

обавести лице о врсти података које се обрађују чак и када их прикупља директно од њега.⁷⁷

1.3. Додатно информисање о обради од стране модела вештачке интелигенције

Када се подаци обрађују коришћењем вештачке интелигенције потребно је пружити све информације које се иначе пружају о обради. Међутим, имајући у виду специфичност овакве обраде, законодавци заузимају став да је потребно укључити и неке додатне информације које нису изричито предвиђене законом за сваку обраду.

На пример, калифорнијски законодавац прописује обавезу да субјекат који развија модел на свом веб сајту упозна јавност са тиме које је скупове података користио за развој и тренинг модела, уз одређене изузетке. То укључује пружање информација о врстама података, да ли скуп тренинг података укључује податке о личности, како подаци доприносе остварењу сврхе за коју се развија модел и да ли су на њима вршене неке измене или обрада.⁷⁸ Поред тога, потребно је пружити и информације о изворима тренинг података, периоду током кога су прикупљени, о томе да ли су купљени или прибављени на основу лиценце, као и о томе да ли су неки од података заштићени ауторским правом, жигом или патентом.⁷⁹ Такође, препоручује се да појединац буде информисан о ризицима који се могу јавити приликом обраде, попут ризика да модел запамти и генерише податке о личности у виду излазног податка.⁸⁰

Додатне обавезе транспарентности у вези са системима вештачке интелигенције су предвиђене и Уредбом ЕУ о вештачкој интелигенцији. Добављачи су према Уредби у обавези да систем развијају тако да појединцу буде очигледно да комуницира са системом вештачке интелигенције, са изузетком система који се користе за одређене сврхе.⁸¹ Поред тога, добављачи треба да осигурају да садржај који генерише систем вештачке интелигенције буде сам по себи обележен као такав, у формату читљивом машинама.⁸² Субјекти који уводе систем су дужни да појединце обавесте о томе да је садржај који се карактерише као уверљив лажан садржај (*deepfake*)⁸³ генерисан или

⁷⁷ Чл. 22. т. 4. Нацрта закона о заштити података о личности.

⁷⁸ Section 3111(a) Cal. Assemb. Bill No. 2013, 2023-2024 Reg. Sess., ch. 817.

⁷⁹ *ibid.*

⁸⁰ Commission Nationale de l'Informatique et des Libertés (CNIL), *IA: Informer les personnes concernées*; преузето 12.07.2026. <https://www.cnil.fr/fr/ia-informer-les-personnes-concernees>.

⁸¹ Art. 50(1) EU AI Act.

⁸² Art. 50(2) EU AI Act.

⁸³ Уверљив лажан садржај (*deepfake*) се у Уредби ЕУ о вештачкој интелигенцији дефинише као „слике, аудио или видео садржај који генерише или којим манипулише вештачка интелигенција, а који наликује

обрађен од стране система вештачке интелигенције.⁸⁴ Ако систем користи биометријске податке за категоризацију лица или препознавање емоција, субјекти који уводе систем морају да представе појединцима начин на који систем функционише.⁸⁵ Потребно је ове информације пружити појединцу најкасније у тренутку његове прве интеракције са моделом или излагања моделу, на јасан и разумљив начин.⁸⁶

Уредба изричито регулише и право на информисаност у вези са одлуком коју на појединца примењује субјект који уводи систем вештачке интелигенције, а која је донета на основу излазних података система. Ово право је ограничено на високоризичне системе, као и на одлуке чије су правне или на сличан начин значајне последице по појединца такве да он сматра да одлука има негативан утицај на његово здравље, сигурност или основна права. Уколико одлука испуњава те услове, појединац може да тражи јасно и разумљиво објашњење главних елемената одлуке и улоге коју је систем имао у поступку њеног доношења.⁸⁷

Нацрт закона о заштити података о личности уводи и обавезу руковооца да информише лице о коришћењу система вештачке интелигенције, укључујући и моделе опште намене. Такво обавештење мора бити пружено на јасан и приступачан начин, најкасније у тренутку прве интеракције са системом или првог излагања садржаја.⁸⁸ Поред тога, уводи се и обавеза руковооца и обрађивача да означе садржај који је генерисао или модификовао модел вештачке интелигенције.⁸⁹ Изузетак од ове обавезе предвиђен је у случају система који је намењен откривању и гоњењу учиниоца кривичног дела.⁹⁰

1.4. Нејасноће у законским одредбама

Постоје одређене нејасноће у формулацији коју користе и ЗЗПЛ и GDPR које нису изричито појашњене у самом тексту закона. Наиме, све наведене информације које треба пружити прописане су у по два става у члановима 23. и 24. ЗЗПЛ, као и у члановима 13. и 14. GDPR-а. Оба закона праве разлику између та два става, на сличан начин наводећи

стварним особама, предметима, местима, субјектима или догађајима и који би се неке лажно чинио веродостојним или истинитим“ (Art. 3(60) EU AI Act).

⁸⁴ Art. 50(4) EU AI Act.

⁸⁵ Art. 50(3) EU AI Act.

⁸⁶ Art. 50(5) EU AI Act.

⁸⁷ Art. 86(1) EU AI Act.

⁸⁸ Чл. 53. ст. 2. и 3. Нацрта закона о заштити података о личности.

⁸⁹ Чл. 53. ст. 6. Нацрта закона о заштити података о личности.

⁹⁰ *ibid.*

да се информације из става 2. морају пружити уколико су неопходне да се обезбеди поштена и транспарентна обрада. На основу овако формулисаног услова може се поставити питање када би се могло сматрати да постоји таква неопходност пружања информација.

Нацртом закона о заштити података о личности се у вези са овим питањем дефинише обим одговорности руковоаца за транспарентну обраду. Наиме, према Нацрту закона сматраће се да је обрада транспарентна ако је руководалац предузео одговарајуће мере да лице информиса о обради, као и о остваривању других права прописаних законом у вези са обрадом.⁹¹ Оваквом одредбом би се могла отклонити сумња макар око тога да ли лице у сваком случају треба да буде информисано о својим правима.

У одсуству изричитог тумачења овог питања, потребно је узети у обзир одговорност руковоаца за транспарентност обраде прописану чланом 5. ЗЗПЛ, као и чињеницу да је терет доказивања такве обраде на руковоацу.⁹² Став Радне групе из члана 29. је да се све информације морају пружити лицу, изузев оних које је у конкретном случају немогуће пружити због тога што нису применљиве или не постоје.⁹³ Најсигурнији приступ до даљег развоја закона је пружити све прописане информације из оба члана, како би ризик неусаглашености са законом био што мањи.

Поред тога, може се јавити дилема око тога како је регулисано информисање о изведеним подацима које је модел сам створио. Наиме, појединца у том случају треба информисати о томе да ће се његови подаци користити у сврху стварања изведених података, као и њиховим категоријама и сврси њиховог даљег коришћења. С обзиром на то да се информације пружају приликом прикупљања података, постоји хипотетичка могућност да руководалац неће у том тренутку знати да ће на основу прикупљених података настати нови, изведени подаци, или да неће знати које ће категорије изведених података бити створене. Тада би се руководалац морао осврнути на одредбу којом му се налаже да пружи информације о даљој обради ако податке о личности обрађује за сврху различиту од првобитне.⁹⁴

⁹¹ Чл. 21. ст. 1. Нацрта закона о заштити података о личности.

⁹² Повереник за информације од јавног значаја и заштиту података о личности. *Заштита података о личности: Ставови, мишљења и пракса Повереника, Публикација бр. 10*, Београд, 2025, стр. 99.

⁹³ Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679*, op. cit.

⁹⁴ *ibid.*

Још једна дилема може настати у случају када се изведени подаци стварају на основу података који се не сматрају подацима о личности, а изведени подаци сами по себи представљају податке о личности. Уопштено, закон предвиђа информисање лица у случају када се подаци прикупљају директно од њега, као и када се не прикупљају од њега. Дакле, постоји изричито регулисање ситуација у којима постоји прикупљање података, али не и ситуације када руковалац сам ствара податке о личности, где нема прикупљања података у правом смислу те речи.⁹⁵ Решење се може наћи у телеолошком тумачењу одредби закона којима се прописује право на информисаност, које се може аналогијом извести и из праксе Суда правде Европске уније,⁹⁶ чиме би се опсег овог права проширио и на обраду изведених података.⁹⁷ Такво тумачење подржава и Радна група из члана 29, која изведене податке сматра за „нове податке о личности који нису непосредно прибављени од лица на које се односе“.⁹⁸ Ова формулација указује на то да би се изведени подаци могли сврстати у податке који су обухваћени чланом 24. ЗЗПЈ и чланом 14. GDPR-а. Свакако, потребно је прецизно тумачење како би се отклонила свака сумња.

1.5. Изузеци од обавезе непосредног информисања лица о обради

Из текста закона произилази да руковалац информације пре свега треба директно да пружи лицу чије податке обрађује. У одређеним ситуацијама, лично информисање лица о обради може бити нецелисходно или захтевати непропорционалан напор од руковаоца. На пример, ако подаци нису прикупљени директно од појединца, обавештавање сваког појединца лично може изискивати несразмеран трошак, па чак и бити немогуће. Овакав случај се може јавити када руковалац прикупља велику количину података за тренинг модела вештачке интелигенције из више различитих извора. Тада се руковаоцу дозвољава да ову обавезу испуни тако што ће јавно објавити све неопходне информације о обради, уз друге одговарајуће мере заштите права и слобода појединаца.⁹⁹ На тај начин ће те информације бити лако доступне сваком лицу. Свакако је важно имати у виду да је потребно појединца упућивати на јавно доступно обавештење о обради када год је то

⁹⁵ S. Wachter, B. Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, *Columbia Business Law Review*, Vol. 2019(2), p. 545.

⁹⁶ Case C-634/21, *OQ v Land Hessen*, intervener: *SCHUFA Holding AG (SCHUFA Holding and Others)*, para. 57.

⁹⁷ B. Custers, H. Vrabec, Tell me something new: data subject rights applied to inferred data and profiles, *Computer Law & Security Review*, Vol. 52, p. 7.

⁹⁸ Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*; преузето 14.09.2026.

<https://ec.europa.eu/newsroom/article29/items/612053>

⁹⁹ Чл. 24. ст. 5. т. 2. ЗЗПЈ; Art. 14(5)(b) GDPR.

могуће. Обрада се не би могла сматрати транспарентном ако је обавештење о обради „сакривено“ на веб сајту руковођаца, као и ако руковођац оствари контакт са лицем на које се подаци односе а не искористи прилику да га упуту на информације о обради. Такође, руковођац мора да буде у стању да докаже да би непосредно обавештавање сваког појединца изискивало количину напора која претеже над последицама које по њих могу наступити уколико нису непосредно обавештени.

Уколико је лице већ обавештено о обради и упознато са свим прописаним информацијама, руковођац нема обавезу да га поново обавештава о њима.¹⁰⁰ Поред тога, може се десити да је обрада изричито прописана законом који истовремено обезбеђује одговарајуће мере заштите легитимних интереса лица на која се подаци односе. Такође, може постојати обавеза чувања поверљивости података у складу са законом или обавезом чувања професионалне тајне. У тим ситуацијама руковођац ће бити дужан да лице обавести о обради само уколико је податке прикупио директно од њега.¹⁰¹

Већина компанија које развијају велике моделе вештачке интелигенције се ослања на изузетке од обавезе директног обавештавања лица, с обзиром на количину тренинг података различитих појединаца које прикупљају. Па ипак, треба имати у виду да је у свакој ситуацији потребна појединачна анализа оправданости ослањања на изузетке. У питању су правила која се примењују од случаја до случаја.¹⁰²

Подаци за учење модела се, између осталог, могу прикупити тако што веб робот (*web crawler*) претражује интернет и прикупља податке, што је познатије као „*web scraping*“. Уколико руковођац информисе лица о оваквој обради путем јавно доступног обавештења, у њему је потребно прецизно навести изворе података. Ако то није у потпуности изводљиво, потребно је назначити које врсте извора нису наведене и због чега, као и да ли су оне јавно доступне. Било би сврсисходно и омогућити лицима да претражују листу назива домена и интернет адреса сајтова са којих су подаци прикупљени, са назначеним датумом и периодом када су прикупљени. У случају *web scraping*-а, обавештење треба да садржи и карактеристике веб робота.¹⁰³

¹⁰⁰ Чл. 23. ст. 4. и чл. 24. ст. 5. т. 1. ЗЗПЈ; Art. 13(4), 14(5)(a) GDPR.

¹⁰¹ Чл. 24. ст. 5. т. 3. и 4. ЗЗПЈ; Art. 14(5)(c), (d) GDPR.

¹⁰² Commission Nationale de l'Informatique et des Libertés (CNIL), *op. cit.*

¹⁰³ European Data Protection Board, *Guidelines 03/2026 on web scraping in the context of generative AI*; преузето 13.08.2026. https://www.edpb.europa.eu/public-consultations/guidelines-032026-on-web-scraping-in-the-context-of-generative-ai_en#no-back

Приликом прикупљања великог броја података о личности може се десити да руковалац није у стању да идентификује лица на која се подаци односе. Обавештење о обради које због тога учини јавно доступним би требало да садржи и чињеницу да идентификација лица није могућа,¹⁰⁴ као и упућивање на информације које је потребно пружити руковоцу ради идентификације како би могао да испуни захтев појединца, јер у супротном он неће моћи да остварује своја права.¹⁰⁵

1.6. Начин пружања информација

Од руковоца се тражи да информације предочи на „сажет, транспарентан, разумљив и лако доступан начин, коришћењем јасних и једноставних речи, а посебно ако се ради о информацији која је намењена малолетном лицу“.¹⁰⁶ Поред тога, захтева се да се информације пруже у тренутку прикупљања података о личности ако се они прикупљају непосредно од лица,¹⁰⁷ или у законом прописаним роковима ако нису прикупљени непосредно од њега.¹⁰⁸

Приликом пружања информација о обради коју врши модел вештачке интелигенције, руковалац мора да узме у обзир категорије лица којима је намењено обавештење о обради. Индивидуализован приступ омогућава да они заиста разумеју обраду и њене последице. Другим речима, ако се користе подаци појединаца који не разумеју стручни технолошки жаргон, руковалац мора да избегне коришћење компликованих термина и да пружи поједностављено објашњење које не захтева предзнање о технологији која се користи. Ово се нарочито односи на пружање сврсисходних информација о логици која се користи приликом аутоматизованог доношења одлука.

Ни ЗЗПЛ, а ни GDPR, не појашњавају појам „сврсисходних информација о логици која се користи“ (*meaningful information about the logic involved*). Сматра се да би у сваком конкретном случају требало проценити која би се количина информација сматрала „сврсисходном“ за појединца чији се подаци обрађују. Стандард који би се могао

¹⁰⁴ Чл. 20. ст. 2. ЗЗПЛ; Art. 11(2) GDPR.

¹⁰⁵ Commission Nationale de l'Informatique et des Libertés (CNIL), *op. cit.*

¹⁰⁶ Чл. 21. ст. 1. ЗЗПЛ; Art. 12(1) GDPR.

¹⁰⁷ Чл. 23. ст. 1. и 2. ЗЗПЛ; Art. 13(1), (2) GDPR.

¹⁰⁸ Чл. 24. ст. 3. ЗЗПЛ; Art. 14(3) GDPR.

применити је да пружене информације омогуће појединцу да одреди главне факторе који су утицали на донету одлуку и колики је био њихов утицај.¹⁰⁹

Како би појединцу приближио последице обраде, руковалац може користити дијаграме да прикаже како се подаци користе за тренинг модела, како ће модел користити податке након тренинга, као и која је разлика између података за тренинг и излазних података модела као резултата обраде.¹¹⁰ Већина појединаца ће вероватно моћи лакше да разуме визуелни приказ од текстуалног описа.

Информације се могу пружати у фазама уместо одједном ради њиховог лакшег разумевања. У том случају, у првој фази требало би информисати лица о идентитету руковаоца и правима која имају у вези са обрадом. Заинтересованим лицима се може пружити прилика да се детаљније упознају са обрадом у одвојеном обавештењу које би им том приликом било лако доступно.¹¹¹ На пример, када корисник приступи платформи на којој се налази модел, може му искочити прозор који би му пружио основне информације, са линком који би га водио до детаљне Политике приватности руковаоца. Сажетак информација би се такође могао пружити у поздравној поруци коју модел шаље кориснику.¹¹²

Модел вештачке интелигенције често се користе преко платформе на којој корисници имају свој налог или плаћају за услуге коришћења модела. Па ипак, за тренинг модела се углавном неће користити само подаци корисника, већ подаци о личности много ширег круга људи. Проблем се јавља када се обавештење о обради налази на платформи, те је примарно доступно само корисницима. У вези са тим, италијанско надзорно тело *Garante per la protezione dei dati personali* наложило је компанији OpenAI да на адекватан начин информише о обради не само кориснике модела, већ и сва лица чији се подаци могу наћи у скупу тренинг података а која не користе модел. Захтева се да се обавештење о обради пружи на пригодном месту приликом регистрације корисника како би могли да га прочитају пре него што приступе услузи. Такође, *Garante* налаже и спровођење кампање користећи све главне канале комуникације којом би се шира

¹⁰⁹ H. Felzmann, E. F. Villaronga, C. Lutz, A. Tamò-Larrieux, Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns, *Big Data & Society*, Vol. 6(1), p. 3.

¹¹⁰ Commission Nationale de l'Informatique et des Libertés (CNIL), *op. cit.*

¹¹¹ *ibid.*

¹¹² K. Naghiyev, ChatGPT From a Data Protection Perspective, *Baku State University Law Review*, Vol. 10(1), p. 32.

јавност информисала о томе да постоји могућност да су њихови подаци прикупљени и употребљени у сврху унапређења алгоритма. Њоме OpenAI треба и да упутити појединце на обавештење о обради објављено на сајту компаније, као и на могућност да путем алатке на сајту могу затражити брисање својих података о личности.¹¹³

Врста података о личности која се налази у скупу тренинг података такође може диктирати начин испуњења обавезе информисања лица о обради. Када се у скупу података за учење модела могу наћи посебне врсте података о личности, било би најправичније да лица на која се ти подаци односе о томе буду обавештени у разумном временском периоду пре него што модел крене да учи на таквом скупу података. Тиме им се омогућава да остварују своја права пре него што то буде отежано током и након тренинга модела.¹¹⁴

2. Аутоматизовано доношење одлука и профилисање

Најпре, потребно је дефинисати ове појмове како би било јасно какву обраду података о личности обухватају. Аутоматизовано доношење одлука дефинише се као обрада технолошким средствима којом се без учешћа човека доносе одлуке.¹¹⁵ Профилисање је, са друге стране, вид аутоматизоване обраде који доводи до стварања „профила“ лица на које се подаци односе. Важан елемент профилисања је циљ обраде, а то је оцењивање одређеног својства личности појединца, нарочито ради анализе или предвиђања фактора попут учинка на послу, економског положаја, здравственог стања, интереса, понашања или локације.¹¹⁶ Уколико профилисање не укључује доношење одлука, оно подлеже општим правилима заштите података о личности која се односе на сваку обраду. Са друге стране, као засебно регулисано јавља се профилисање којим су без учешћа човека донете одлуке које могу да изазову правне последице или на други начин значајно утичу на положај лица.¹¹⁷

Главно право које појединац има у вези са обрадом која је обухваћена овим појмовима јесте да се на њега не примењује одлука која је донета искључиво на основу

¹¹³ Garante per la protezione dei dati personali, *Provvedimento dell'11 aprile 2023 [9874702]*; преузето 14.07.2026. <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702>

¹¹⁴ Commission Nationale de l'Informatique et des Libertés (CNIL), *op. cit.*

¹¹⁵ Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, *op. cit.*

¹¹⁶ Чл. 4. т. 5. ЗЗПЈ; Art. 4(4) GDPR.

¹¹⁷ Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, *op. cit.*

автоматизоване обраде, ако се њоме производе правне последице по њега, или она значајно утиче на његов положај. То подразумева да ово право треба бити испуњено без обзира на то да ли је појединац поднео захтев за његово остваривање. Самим тим, ову одредбу би требало схватити као општу забрану оваквог доношења одлука, које би било дозвољено само у следећим законом предвиђеним случајевима:¹¹⁸

- одлука је неопходна како би се закључио или извршио уговор чије су уговорне стране лице на које се подаци односе и руковалац,
- одлука је заснована на закону који истовремено прописује одговарајуће мере заштите лица, и
- одлука је заснована на изричитом пристанку појединца.

У овим случајевима, руковалац може применити одлуку, али је истовремено у обавези да предузме одговарајуће мере заштите лица, сем ако оне нису већ прописане законом.

Наведени изузеци нису применљиви у случају обраде посебних врста података о личности. Одлука заснована на овим подацима се може применити само уколико је обрада заснована на изричитом пристанку лица на које се подаци односе, изузимајући ситуације у којима се обрада сама по себи не сме заснивати на пристанку. Поред тога, одлука се може применити и ако је лице податке очигледно учинило јавно доступним. Руковалац у оба случаја има обавезу да усвоји одговарајуће мере заштите лица, мада закон не прописује шта би оне тада најмање требало да укључују.¹¹⁹

Занимљиво је да GDPR уместо ситуације у којој је лице очигледно учинило податке јавно доступним предвиђа да одлука може бити заснована на посебним категоријама података о личности уколико се обрађују ради остварења значајних јавних интереса.¹²⁰ Овакво решење пружа већу заштиту појединцу, јер је обрада посебних врста података који су очигледно учињени јавно доступним сама по себи проблематична и отвара пут бројним могућностима злоупотребе.¹²¹ Чињеница да је лице учинило податак јавно доступним не значи да је тада имало у виду и да ће тај податак можда бити искоришћен како би се донела одлука која би значајно утицала на њега. На пример, појединац би могао на свом јавном профилу на друштвеној мрежи да објави детаље о свом

¹¹⁸ *ibid.*

¹¹⁹ Чл. 38. ст. 4. ЗЗПЛ.

¹²⁰ Art. 22(4) GDPR.

¹²¹ А. Дилигенски, Д. Прља, Д. Церовић, *Право заштите података GDPR*, Београд, 2018, стр. 106.

здравственом стању ради подизања свести о реткој болести коју има. Када би се пријавио за рад у компанији у којој кандидате модел вештачке интелигенције проверава тражећи њихове податке на интернету, могло би доћи до тога да модел аутоматски одбије кандидата због ретке болести коју има, а на основу дискриминаторног закључивања и предрасуда створених током учења модела. Не би било правично дозволити да модел у таквој ситуацији сам одлучује о томе да ли ће лице бити запослено или не.

Мере заштите имају за циљ да у што већој мери омогуће учешће лица у преиспитивању одлуке, с обзиром на значај који она може имати по њега. Оне морају укључивати најмање увођење људског фактора у доношење и преиспитивање одлуке, могућност лица да изрази свој став у вези са њом, као и да је оспори пред овлашћеним лицем руковоаца.¹²² Руковалац би требало да предузме и мере којима би осигурао поштену и транспарентну обраду података, попут коришћења адекватних математичких или статистичких процедура за обраду и мера којима би умањио ризик грешке, повреде права појединца и дискриминаторних последица одлуке.¹²³ Такође, ризик се може умањити и редовним проверама квалитета модела и постојећег ризика дискриминације, као и адекватним тестирањем модела.¹²⁴

Неки законодавци су узели у своје руке да конкретизују обавезе руковоаца у вези са мерама заштите и остваривањем права појединаца у вези са аутоматизованим доношењем одлука. На пример, Уједињено Краљевство је увело процедурална правила којима се појединцима омогућава увид у радње које руковалац предузима како би испунио његов захтев за остваривање права,¹²⁵ док Словенија обавезује руковоаца на спровођење посебне процене утицаја обраде пре него што крене са коришћењем система аутоматизованог доношења одлука.¹²⁶

Модел вештачке интелигенције приликом доношења одлука има приступ много већем броју информација него човек. Услед тога, увођење људског елемента у преиспитивање одлуке може бити отежано. Тамо где је технологија довољно напредовала, ово се може

¹²² Чл. 38. ст. 3. ЗЗПЈ; Art. 22(3) GDPR.

¹²³ Recital 71 GDPR.

¹²⁴ Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, op. cit.

¹²⁵ M. E. Kaminski, J. M. Urban, The Right to Contest AI, *Columbia Law Review*, Vol. 121(7), p. 2021.

¹²⁶ *ibid.*, p. 2042.

олакшати ако је модел сам по себи развијен да омогући транспарентност одлуке.¹²⁷ Уопштено, права предвиђена у вези са аутоматизованим доношењем одлука ослањају се на право на информисаност и транспарентност обраде. Потребно је пружити довољно информација појединцу како би он био у могућности да остварује и друга права која има у вези са одлуком.¹²⁸

У теорији, постоји могућност изврдавања одредби закона тиме што би се увео минимални људски елемент у сам процес одлучивања, тако да се одлука технички не би сматрала донетом искључиво на основу аутоматизоване обраде података.¹²⁹ Предмет теоријске дискусије је и то да ли би ипак било повољније по лица на која се подаци односе да се преиспитивање одлуке повери систему. У будућности је могуће да се модели вештачке интелигенције довољно развију да доносе и преиспитују одлуке узимајући у обзир сва начела правичног одлучивања, а да ризик да одлука буде дискриминаторна и вођена предрасудама буде мањи него што би био у случају када је човек преиспитује.¹³⁰ Постоји и супротно гледиште, према коме би препуштање преиспитивања одлуке моделу вештачке интелигенције отежало могућност откривања предрасуда које су утицале на ту одлуку, с обзиром на то да предрасуде модела могу бити недоступне или нејасне човеку.¹³¹

Нацрт закона о заштити података о личности у потпуности искључује примену права везаних за аутоматизовано доношење одлука и профилисање код обраде података о личности коришћењем вештачке интелигенције.¹³² Са друге стране, забрањује обраду искључиво употребом система вештачке интелигенције без учешћа физичког лица ако то може да произведе штетне последице по лице на које се подаци односе или значајно утиче на његов положај.¹³³

3. Проблем објашњивости модела вештачке интелигенције

Код комплекснијих модела вештачке интелигенције јавља се проблем објашњивости. Појмови „објашњивост“, „транспарентност“ и „интерпретабилност“ имају различита

¹²⁷ European Parliament: Directorate-General for Parliamentary Research Services, *The impact of the general data protection regulation on artificial intelligence*, 2020, p. 60.

¹²⁸ M. E. Kaminski, J. M. Urban, *op. cit.*, p. 1980.

¹²⁹ T. Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, *Seton Hall Law Review*, Vol. 47, p. 1016.

¹³⁰ European Parliament: Directorate-General for Parliamentary Research Services, *op. cit.*, p. 61.

¹³¹ M. E. Kaminski, J. M. Urban, *op. cit.*, p. 2040.

¹³² Чл. 52. ст. 4. Нацрта закона о заштити података о личности.

¹³³ Чл. 53. ст. 4. Нацрта закона о заштити података о личности.

значења у контексту објашњења начина на који модел вештачке интелигенције функционише. „Транспарентност“ подразумева да је доступна она количина информација о моделу и његовим појединачним аспектима и компонентама која дозвољава појединцу да разуме функционисање целог модела. „Интерпретабилност“ постоји када се разлог због ког је модел донео одлуку може јасно разумети због тога што је разумљив конкретан начин на који он функционише. „Објашњивост“ се такође фокусира на разумевање разлога иза одређене одлуке и обухвата интерпретабилност, али у објашњење укључује и друге факторе поред начина функционисања модела, као што су етичка питања и комуникација корисника са моделом.¹³⁴ На пример, модел би могао бити транспарентан ако је доступна детаљна техничка документација о њему и све неопходне информације о обради, интерпретабилан ако је у техничкој документацији могуће довољно јасно представити начин његовог функционисања, и објашњив ако је могуће разумети како су фактори као што су интеракција корисника и потенцијалне предрасуде утицали на донету одлуку.

Према томе колико су објашњиви, моделе вештачке интелигенције можемо поделити на моделе „беле кутије“ (*white box models*) и „црне кутије“ (*black box models*). Модели „беле кутије“ су сами по себи објашњиви због начина на који функционишу. Они на прилично једноставан и транспарентан начин уче, закључују и доносе одлуке, а уз то је и јасно које варијабле су утицале на коначну одлуку. У ову групу спадају, на пример, стабло одлучивања (*decision tree*) и линеарна регресија.¹³⁵

Са друге стране, модели „црне кутије“, попут неуронских мрежа, функционишу на веома комплексан начин. Ни руковалац није у стању да у потпуности разуме како долазе до одређеног закључка, а ни сам модел не може то да образложи. Иако улазне варијабле могу бити познате, то не значи да је могуће одредити које су од тих улазних варијабли утицале на одлуку.¹³⁶ Код модела „црне кутије“, објашњење модела се може дати тек након што је одлука донета.¹³⁷ Постоји мишљење да се овакво *post-hoc* објашњење ипак

¹³⁴ European Data Protection Supervisor, *TechDispatch* #2/2023 - *Explainable Artificial Intelligence*; преузето 17.08.2026. https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-22023-explainable-artificial-intelligence_en

¹³⁵ *ibid.*

¹³⁶ Закључак о усвајању Етичких смерница за развој, примену и употребу поуздане и одговорне вештачке интелигенције, *Службени гласник РС*, бр. 23/2023-19.

¹³⁷ European Data Protection Supervisor, *op. cit.*

не може сматрати довољно поузданим, као и да може довести до тога да појединац погрешно верује да је одлука оправдано донета, иако то није нужно случај.¹³⁸

Проблем објашњивости модела „црне кутије“ не ствара само потешкоће руковооцу у испуњавању његових законских обавеза, већ и појединцу у разумевању могућности да остварује своја права. Другим речима, ако појединцу није лако да разуме да је неку одлуку донео модел вештачке интелигенције, као ни на основу којих података је она донета, он неће моћи да установи да ли су у питању нетачни подаци у вези са којима има право исправке, као и да ли је у питању одлука која је донета искључиво на основу аутоматизоване обраде, а за коју има право да се не примењује на њега.¹³⁹

¹³⁸ S. Bordt, M. Finck, E. Raidl, U. von Luxburg, Post-Hoc Explanations Fail to Achieve Their Purpose in Adversarial Contexts; in: *FACCT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, Seoul, 2022, Association for Computing Machinery, p. 903.

¹³⁹ L. Edwards, M. Veale, Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”?, *IEEE Security & Privacy*, Vol. 16(3), p. 50.

IV ПРАВО НА ПРИСТУП И ПРЕНОСИВОСТ ПОДАТАКА

Право на приступ подацима и преносивост података донекле су подударна у томе што омогућавају лицу да од руковоаца затражи своје податке о личности. Ово поглавље излаже садржај ових права, разлике између њих и могућност њиховог остваривања у контексту вештачке интелигенције.

1. Право на приступ

Право на приступ подацима се може схватити као допуна права на информисаност, нарочито у ситуацијама када се лица на која се подаци односе не обавештавају непосредно о обради. Када руковалац испуњава обавезу информисања лица, он му у тренутку прикупљања података даје информације о томе како планира да их обрађује. Путем захтева за приступ појединац може у каснијим стадијумима обраде да добије информације које приказују истинито стање.¹⁴⁰ Њиме се омогућава да појединац, пре свега, тражи информацију о томе да ли се његови подаци обрађују.¹⁴¹ Ако је одговор потврдан, може тражити и детаљније информације о обради које су у одређеној мери подударне са садржајем права на информисаност. Самим тим, дилеме које се могу јавити у вези са правом на информисаност када обраду врши вештачка интелигенција могу се јавити и у случају права на приступ, у оном обиму у коме су ова два права подударна. Потребно је имати у виду да она свакако нису међусобно искључива.

Наиме, лице има право да тражи детаље о сврси обраде,¹⁴² врстама података о личности који се обрађују¹⁴³ и извору из кога су прикупљени ако нису прикупљени непосредно од њега.¹⁴⁴ Поред тога, има право да тражи да га руковалац обавести о примаоцима или категоријама прималаца података, нарочито онима који се налазе у другим земљама или међународним организацијама,¹⁴⁵ периоду чувања података или критеријумима на основу којих се он одређује¹⁴⁶ и одређеним правима које има у односу на обраду,¹⁴⁷ укључујући и право да се поднесе притужба Поверенику, односно другом надлежном надзорном телу.¹⁴⁸ Захтевом се може тражити и информација о постојању

¹⁴⁰ B. Custers, H. Vrabec, *op. cit.*, p. 7.

¹⁴¹ Чл. 26. ст. 1. ЗЗПЈ; Art. 15(1) GDPR.

¹⁴² Чл. 26. ст. 1. т. 1. ЗЗПЈ; Art. 15(1)(a) GDPR.

¹⁴³ Чл. 26. ст. 1. т. 2. ЗЗПЈ; Art. 15(1)(b) GDPR.

¹⁴⁴ Чл. 26. ст. 1. т. 7. ЗЗПЈ; Art. 15(1)(g) GDPR.

¹⁴⁵ Чл. 26. ст. 1. т. 3. ЗЗПЈ; Art. 15(1)(c) GDPR.

¹⁴⁶ Чл. 26. ст. 1. т. 4. ЗЗПЈ; Art. 15(1)(d) GDPR.

¹⁴⁷ Чл. 26. ст. 1. т. 5. ЗЗПЈ; Art. 15(1)(e) GDPR.

¹⁴⁸ Чл. 26. ст. 1. т. 6. ЗЗПЈ; Art. 15(1)(f) GDPR.

автоматизованог доношења одлука, као и сврсисходне информације о логици иза њега, значају и очекиваним последицама обраде на појединца.¹⁴⁹ Ако постоји пренос података у другу државу или међународну организацију, могу се тражити и информације о постојећим мерама заштите.¹⁵⁰ Руковалац је дужан да појединцу на захтев омогући приступ његовим подацима које обрађује¹⁵¹ и достави копије тих података.¹⁵² У сваком случају, достављањем копије се не сме угрозити остваривање права и слобода других лица.¹⁵³ То обухвата пословне тајне и права интелектуалне својине, нарочито ауторско право којим се штити рачунарски програм,¹⁵⁴ али и сва друга права предвиђена применљивим законима.¹⁵⁵ Уколико се установи да би достављање копија података имало негативан утицај на права или интересе трећих лица, потребно је пронаћи начин да се тај негативан утицај отклони или умањи до оне мере где би интерес лица које тражи приступ подацима постао претежан.

Нацрт закона о заштити података о личности предлаже одредбу којом се право на приступ подацима у случају обраде коришћењем вештачке интелигенције¹⁵⁶ може ограничити ако би то значајно отежало остваривање сврхе, или ако руковалац не може да идентификује то лице.¹⁵⁷ Како би се осигурала прецизност, овај изузетак би могао изричито предвиђати и могућност лица да достави додатне податке који би омогућили идентификацију и самим тим остваривање права, као што је већ предвиђено код обраде која не захтева идентификацију.¹⁵⁸

Прва копија података коју руковалац доставља појединцу мора бити достављена без накнаде.¹⁵⁹ Ако лице тражи додатне копије, а њихова израда изискује одређене нужне трошкове, руковалац може захтевати да му буду надокнађени.¹⁶⁰ Трошкови треба да буду

¹⁴⁹ Чл. 26. ст. 1. т. 8. ЗЗПЈ; Art. 15(1)(h) GDPR.

¹⁵⁰ Чл. 26. ст. 2. ЗЗПЈ; Art. 15(2) GDPR.

¹⁵¹ Чл. 26. ст. 1. ЗЗПЈ; Art. 15(1) GDPR.

¹⁵² Чл. 26. ст. 3. ЗЗПЈ; Art. 15(3) GDPR.

¹⁵³ Чл. 26. ст. 4. ЗЗПЈ; Art. 15(4) GDPR.

¹⁵⁴ Recital 63 GDPR.

¹⁵⁵ European Data Protection Board, *Guidelines 01/2022 on data subject rights - Right of access*; преузето 03.10.2026. https://www.edpb.europa.eu/system/files/documents/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

¹⁵⁶ „Обрада података о личности коришћењем вештачке интелигенције“ је обрада у сврхе „примене, укључујући развој и тестирање система вештачке интелигенције, као и модела вештачке интелигенције опште намене“ (Чл. 52. ст. 1. Нацрта закона о заштити података о личности).

¹⁵⁷ Чл. 52. ст. 3. Нацрта закона о заштити података о личности.

¹⁵⁸ Чл. 20. ст. 3. ЗЗПЈ.

¹⁵⁹ Чл. 21. ст. 5. ЗЗПЈ; Art. 12(5) GDPR.

¹⁶⁰ Чл. 26. ст. 3. ЗЗПЈ; Art. 15(3) GDPR.

разумни и сведени на нужни минимум, а лице треба да буде упућено на износ накнаде трошкова пре него што затражи додатну копију.¹⁶¹ Информације је потребно доставити у уобичајено коришћеном електронском облику ако је појединац доставио захтев електронским путем, сем ако није тражио другачије достављање.¹⁶² Када је то могуће, појединцу би требало омогућити непосредан приступ подацима путем сигурних канала.¹⁶³ У случају вештачке интелигенције, потребно је наћи најефикаснији канал обезбеђен мерама које омогућавају приступ искључиво подацима који се односе на конкретно лице. То може бити тешко код великих база података, те је важно и саму базу података од почетка пројектовати на начин који омогућава филтрирање и селективан приказ података.

Начин на који ЗЗПЛ регулише достављање информација на основу захтева упућеног у електронском облику може изазвати дилеме јер користи израз „захтев за копију“, што се може схватити као да се односи само на копију података о личности, а не и на информације о обради. Излажући одредбе закона у предметима у којима је одлучивао, Повереник је истакао да је руковалац дужан да „лицу које је поднело захтев електронским путем пружи информацију у електронском облику уколико је то могуће“.¹⁶⁴ Могуће је да се Повереник том приликом ослања на општу обавезу руковаоца да лицима на основу захтева у вези са остваривањем њихових права пружи информације у електронском облику, ако је то погодно.¹⁶⁵ Са друге стране, GDPR се не ограничава на захтев за копију већ користи израз „захтев“, те се одредба може схватити као да се односи на било какву садржину захтева обухваћену овим правом. Овакву формулацију спорне одредбе би требало да прихвати и ЗЗПЛ. Нацрт закона о заштити података о личности наизглед пружа решење ове дилеме, предвиђајући да се информација о обради може дати и електронским путем.¹⁶⁶ У сваком случају, разумно је сматрати да је погодно да информације и подаци буду пружени у електронском облику када обраду врши вештачка интелигенција.

¹⁶¹ European Data Protection Board, *Guidelines 01/2022 on data subject rights - Right of access*, *op. cit.*

¹⁶² Чл. 26. ст. 3. ЗЗПЛ; Art. 15(3) GDPR.

¹⁶³ Recital 63 GDPR.

¹⁶⁴ Повереник за информације од јавног значаја и заштиту података о личности, *Заштита података о личности: Ставови и мишљења Повереника, Публикација бр. 6*, Београд, 2021, стр. 82.

¹⁶⁵ Чл. 21. ст. 1. ЗЗПЛ.

¹⁶⁶ Чл. 54. ст. 3. Нацрта закона о заштити података о личности.

Разлог због кога појединац тражи приступ подацима и информацијама о обради не сме бити чињеница на основу које руковалац може да одбије пружање информација. Чак и ако руковалац сматра да ће те информације бити искоришћене на његову штету, на пример, да ће појединац те информације употребити пред судом у поступку против руковаоца, он је свакако дужан да испуни његов захтев.¹⁶⁷

2. Право на преносивост података о личности

Право на преносивост има велики значај у добу када су доступне различите платформе које пружају исте услуге. Тиме што је појединцу олакшан пренос података између платформи, омогућава му се слободан избор платформе коју ће користити, што отежава услове за стварање монопола одређених руковалаца. Правом на преносивост се, дакле, омогућава већа контрола појединаца над њиховим подацима о личности, а уједно се остварују и шири друштвени интереси, попут подстицања конкуренције.¹⁶⁸ Може се изнети и супротан аргумент према коме право на преносивост може довести до неправичне праксе компанија, јер ће мањим компанијама бити на тај начин много лакше да дођу до података које су веће компаније већ прикупиле.¹⁶⁹

Ово право може се упоредити са правом на приступ подацима, с обзиром на то да оба права омогућавају лицу да затражи и добије своје податке о личности. Суштина права на преносивост, за разлику од права на приступ, је да се ти подаци пруже у структурисаном, уобичајено коришћеном и електронски читљивом облику. То омогућава појединцу да их лако пренесе другом руковаоцу ако то жели, а притом може захтевати од првобитног руковаоца да га у томе не омета.¹⁷⁰ Може се тражити и директан пренос другом руковаоцу, што ће првобитни руковалац морати да испуни само ако је то технички изводљиво.¹⁷¹

Још једна разлика у односу на право на приступ подацима је у томе што је право на преносивост признато лицима само ако су испуњени законом предвиђени услови. Потребно је да се траже подаци које је лице претходно доставило руковаоцу, што значи да се подаци које је руковалац прибавио од трећих лица не могу обухватити овим захтевом. Међутим, може се јавити дилема око тога да ли би то обухватило и податке

¹⁶⁷ European Data Protection Board, *Guidelines 01/2022 on data subject rights - Right of access*, *op. cit.*

¹⁶⁸ С. Андоновић, Д. Прља, *Основи права заштите података о личности*, Београд, 2020, стр. 108.

¹⁶⁹ М. Humerick, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *Santa Clara High Technology Law Journal*, Vol. 34(4), p. 409.

¹⁷⁰ Чл. 36. ст. 1. ЗЗПЈ; Art. 20(1) GDPR.

¹⁷¹ Чл. 36. ст. 2. ЗЗПЈ; Art. 20(2) GDPR.

које је руковалац сам прикупио од лица, на пример, праћењем његовог понашања.¹⁷² Имајући у виду циљ права на преносивост, као и то да се све чешће на тај начин прикупљају подаци о личности кључни за сврху обраде, чини се да би правично решење било да захтев може да обухвати и такве податке. Такав став заузела је и Радна група из члана 29.¹⁷³

Поред тога, пренос података се може тражити само ако је основ за њихову обраду био пристанак или уговор, уз кумулативно испуњење услова да се обрада врши аутоматизовано.¹⁷⁴ Најзад, потребно је и да остварење овог права нема штетан утицај на остваривање права и слобода других лица.¹⁷⁵

Проблем се може јавити услед тога што се приликом стварања изведених података може сматрати да их појединац није претходно доставио руковоцу и да самим тим не могу бити обухваћени захтевом за преносивост.¹⁷⁶ Због тога је потребно пронаћи решење којим би се проширио опсег овог права на изведене податке.

Према Нацрту закона о заштити података о личности, лица не би имала право да захтевају пренос података код обраде података о личности коришћењем вештачке интелигенције.¹⁷⁷

¹⁷² European Parliament: Directorate-General for Parliamentary Research Services, *op. cit.*, p. 57.

¹⁷³ Article 29 Data Protection Working Party, *Guidelines on the right to data portability*; преузето 06.10.2026. <https://ec.europa.eu/newsroom/article29/items/611233>

¹⁷⁴ Чл. 36. ст. 1. ЗЗПЈ; Art. 20(1) GDPR.

¹⁷⁵ Чл. 36. ст. 4. ЗЗПЈ; Art. 20(4) GDPR.

¹⁷⁶ B. Custers, H. Vrabec, *op. cit.*, p. 11.

¹⁷⁷ Чл. 52. ст. 4. Нацрта закона о заштити података о личности.

V ПРАВО НА ИСПРАВКУ И БРИСАЊЕ ПОДАТАКА

Ово поглавље посвећено је правима која лице има у вези са исправком или допуном и брисањем података о личности. Посебна пажња посвећује се остваривању ових права у односу на изведене податке и утицај који податак о личности оствари на модел током процеса учења.

1. Право на исправку и допуну

С обзиром на то да модел вештачке интелигенције, између осталог, закључивањем изводи нове податке из података о личности које обрађује, важно је да закључци које донесе буду утемељени на тачним и потпуним подацима о личности. Право на исправку и допуну омогућава појединцу да то осигура. Од руковоаца се може тражити исправка нетачних података, али и допуна непотпуних података, за шта може бити потребно и давање додатне изјаве.¹⁷⁸ Остваривање овог права може се повезати и са правом на ограничење обраде, јер се обрада може ограничити у року потребном да руковалац провери тачност података о личности.¹⁷⁹ Уколико је руковалац делио податке са другим субјектима, потребно је да све примаоце обавести о томе да је дошло до исправке или допуне података, изузев ако би то изискивало прекомеран утрошак времена и средстава.¹⁸⁰ Појединац има право и да тражи да буде информисан о тим примаоцима.¹⁸¹

Право на исправку и допуну применљиво је и на улазне и на излазне податке, те закључци и други изведени подаци у теорији могу бити предмет захтева за исправку.¹⁸² Када су подаци о личности доказиве чињенице, разумно је сматрати да је потребно да се може доказати да је податак нетачан или непотпун како би се могла тражити исправка или допуна.¹⁸³ Међутим, изведени подаци се налазе у „сивој“ зони и њихова тачност није лако доказива, а некада је и потпуно немогућа.¹⁸⁴ На пример, тачност неких предвиђања се може доказати тек када се она остваре,¹⁸⁵ док тачност закључака може бити

¹⁷⁸ Чл. 29. ЗЗПЈ; Art. 16 GDPR.

¹⁷⁹ Чл. 31. ст. 1. т. 1. ЗЗПЈ; Art. 18(1)(a) GDPR.

¹⁸⁰ Чл. 33. ст. 1. ЗЗПЈ; Art. 19 GDPR.

¹⁸¹ Чл. 33. ст. 2. ЗЗПЈ; Art. 19 GDPR.

¹⁸² Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, op. cit.

¹⁸³ S. Wachter, B. Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, op. cit., p. 548.

¹⁸⁴ Case C-460/20, *Google (Déréfèrencement d'un contenu prétendument inexact)*, para. 66.

¹⁸⁵ A. Häuselmann, B. Custers, The Right to Rectification and Inferred Personal Data, *European Journal of Law and Technology*, Vol. 15 (3), p. 2.

субјективна.¹⁸⁶ Руковалац може, на пример, сматрати да је изведени податак тачан упркос тврдњи појединца, узимајући у обзир статистичке методе којима се дошло до тог податка и њихове маргине грешака, те тада може бити упитно чија ће се интерпретација сматрати валидном.¹⁸⁷ Право лица да тражи исправку таквих података о личности је отежано због тога што би се могло сматрати да је на њему терет доказивања да је податак нетачан.¹⁸⁸ На пример, OpenAI захтева од појединца да објасни зашто је одређени податак о личности нетачан, као и да за то достави поуздане доказе.¹⁸⁹

Па ипак, треба имати у виду да изведени подаци могу сами по себи спадати у посебне категорије података о личности, или настати на основу података који спадају у те категорије. Може се десити и да изведен податак настане под утицајем предрасуда које модел има приликом закључивања. У таквим случајевима је нарочито важно да лице има могућност да исправи нетачан закључак о себи.¹⁹⁰ Један од начина на који се могу категорисати изведени подаци чија тачност се не може прецизно утврдити је да се сматрају „обмањујућим“ у смислу тога да погрешно приказују стварност. На тај начин би се они могли сврстати у непотпуне податке који захтевају додатне информације и допуну како би на исправан начин приказали стварност.¹⁹¹

Исправљање улазних података на основу којих је настао изведени податак неће у потпуности осигурати тачност изведеног податка, али јој свакако може допринети.¹⁹² Па ипак, и даље је отворено питање у којој мери је заправо могуће извршити исправку податка на коме се модел учио. Руковаоци попут Anthropic-a¹⁹³ и SpaceXAI-a¹⁹⁴ у својим Политикама приватности напомињу да услед сложености модела постоји могућност да неће моћи да испуне захтев за остваривање права на исправку.

¹⁸⁶ *ibid.*, p. 3.

¹⁸⁷ B. Custers, H. Vrabec, *op. cit.*, p. 9.

¹⁸⁸ A. Häuselmann, B. Custers, *op. cit.*, p. 2.

¹⁸⁹ OpenAI, *Right to be forgotten and personal data removal from ChatGPT*; преузето 06.10.2026. <https://help.openai.com/en/articles/20001057-right-to-be-forgotten-and-personal-data-removal-from-chatgpt>

¹⁹⁰ B. Fernández Delgado, V. Cazorro Barahona, *op. cit.*, p. 7.

¹⁹¹ R. Silva Gomes, Data subject rights in the era of AI. Can the right of rectification protect data subjects against incorrect inferences made by artificial intelligence systems?, *Quaderns IEE: Revista de l'Institut d'Estudis Europeus*, Vol. 4(2), p. 91.

¹⁹² A. Häuselmann, B. Custers, *op. cit.*, p. 10.

¹⁹³ Anthropic, *Privacy Policy*; преузето 06.10.2026. <https://www.anthropic.com/legal/privacy>

¹⁹⁴ SpaceXAI, *SpaceXAI's Europe Privacy Policy Addendum*; преузето 06.10.2026. <https://x.ai/legal/europe-privacy-policy-addendum>

Нацрт закона о заштити података о личности у потпуности искључује примену овог права код обраде података о личности коришћењем вештачке интелигенције.¹⁹⁵

2. Право на брисање

Право појединца да у одређеним случајевима захтева да буде „заборављен“ извео је Суд правде Европске уније у случају *Google Spain*.¹⁹⁶ GDPR је формализовао ово право у виду права на брисање података о личности, а као таквог га предвиђа и ЗЗПЛ. Важно је напоменути да је ово право постављено рестриктивно. Појединац увек може да тражи брисање својих података о личности, али ће руковалац бити у обавези да их избрише само у тачно одређеним случајевима:¹⁹⁷

- подаци више нису неопходни како би се оствариле сврхе због којих су обрађивани,
- руковалац има законску обавезу да избрише податке,
- лице је опозвало свој пристанак и не постоји други правни основ за обраду,
- лице је уложило приговор на обраду, а нема другог правног, или, у случају GDPR-а, легитимног основа за обраду који претеже над његовим правима и интересима,
- лице је уложило приговор на обраду за потребе директног оглашавања,
- обрада је незаконита,
- подаци су прикупљени у вези са коришћењем услуга информационог друштва од стране малолетних лица.

Руковалац треба да обавести о брисању података о личности све примаоце тих података, изузев ако је то немогуће или изискује прекомерне трошкове, као и да лице на захтев информише о тим примаоцима.¹⁹⁸ Уколико је руковалац учинио податке јавно доступним, има обавезу да предузме све разумне мере да и други руковаоци који их обрађују обришу те податке. Потребно је у те сврхе обавестити друге руковаоце да је поднет захтев за брисање и да је потребно да се обришу и све копије, као и електронске везе и упућивања ка овим подацима. Како би испунио ову обавезу, руковалац може предузети и одговарајуће техничке мере, узимајући у обзир доступне технологије и трошкове које би њихова употреба изискивала.¹⁹⁹

¹⁹⁵ Чл. 52. ст. 4. Нацрта закона о заштити података о личности.

¹⁹⁶ Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.

¹⁹⁷ Чл. 30. ст. 2. ЗЗПЛ; Art. 17(1) GDPR.

¹⁹⁸ Чл. 33. ЗЗПЛ; Art. 19 GDPR.

¹⁹⁹ Чл. 30. ст. 3. ЗЗПЛ; Art. 17(2) GDPR.

Изузеци од примене овог права односе се на обраду која је неопходна ради остваривања слободе изражавања и информисања, испуњења законских обавеза руковоаца, вршења послова у јавном интересу или службених овлашћења руковоаца, остваривања јавног интереса у области јавног здравља, као и подношења, остваривања или одбране правног захтева. Изузетак постоји и када се подаци обрађују у сврхе архивирања у јавном интересу, сврхе научног или историјског истраживања, као и статистичке сврхе, ако је оправдано очекивати да би остваривање права могло да онемогући или битно угрози остваривање тих сврха.²⁰⁰ Руковаоци су се можда могли позивати на сврхе научног истраживања у почетним фазама развоја вештачке интелигенције,²⁰¹ али је то теже сада када се већина модела користи и у комерцијалне сврхе.²⁰²

Када се разматра примена овог права на обраду коју врши модел вештачке интелигенције, главно питање које се поставља је начин тумачења појма „брисање“. Ако би се овај појам тумачио у строго језичком смислу, „брисање“ би се схватило као потпуно уклањање податка о личности. Овако протумачен појам брисања је тешко применљив у контексту модела вештачке интелигенције из више разлога. Проблематика у примени потпуног брисања података у комплексним технологијама обраде података је представљала дилему и приликом доношења GDPR-а, с обзиром на то да је постојао предлог одредбе којом би се дозволило ограничење уместо брисања податка. Па ипак, чињеница да та одредба није постала део коначног законског текста значи да се техничке потешкоће не могу саме по себи сматрати за легитиман разлог одбијања испуњења захтева за брисање.²⁰³

Базе података на којима се темељи рад модела вештачке интелигенције садрже више копија истог податка о личности како би систем могао да се врати у пређашње стање у случају непредвиђених догађаја. Ради потпуног уклањања податка, било би потребно идентификовати и уклонити сваку његову копију, што би изискивало значајне трошкове

²⁰⁰ Чл. 30. ст. 5. ЗЗПЈ; Art. 17(3) GDPR.

²⁰¹ K. Naghiyev, *op. cit.*, p. 22.

²⁰² D. Zhang, P. Finckenberg-Broman, T. Hoang, S. Pan, Z. Xing, M. Staples, X. Xu, Right to Be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions, *AI and Ethics*, Vol. 5(3), p. 2449.

²⁰³ K. Hawkins, N. Alhuwaish, S. Belguith, A. Vranaki, A. Charlesworth, A Decision-Making Process to Implement the 'Right to Be Forgotten' in Machine Learning; in: Rannenberg K., Drogkaris P. and Lauradoux C., (eds.), *Privacy Technologies and Policy - APF 2023, Lyon, France, June 1–2, 2023, Proceedings*, Cham, 2024, p. 27.

за руковоаца.²⁰⁴ Потпуно уклањање податка и поновно тренирање модела након тога може потрајати месецима.²⁰⁵

Постоје и дилеме око тога који ће све подаци морати да буду избрисани и шта ће бити домашај овог права. На пример, поставља се питање да ли би брисање неког податка о личности требало да узрокује и брисање података који су изведени из њега у виду закључака и предвиђања. Требало би омогућити брисање изведених података из више разлога. Најпре, то је важно ако је разлог подношења захтева за брисање чињеница да је обрада од самог почетка незаконита.²⁰⁶ Затим, као што је случај и са правом на исправку и допуну података, изведени податак или подаци на основу којих је настао могу спадати у посебне врсте података о личности. На крају, ако је закључак донет под утицајем предрасуда, право на брисање би требало да обухвати и додатно или поновно учење модела како те предрасуде не би утицале на изведени податак приликом наредног закључивања.²⁰⁷

Дилема се јавља и у вези са тим да ли би појединац могао да тражи брисање утицаја његовог податка о личности насталог током учења модела, иако податак није сачуван у свом изворном облику. Утицај податка јавља се у виду „тежина“ (*weights*) које утичу на закључивање модела и које чине његов нераскидиви део, те би то изискивало значајне трошкове и угрозило ефикасност модела.²⁰⁸ Поред тога, потпуно брисање податка неће нужно уклонити сваку могућност његовог поновног појављивања у виду излазне вредности модела, с обзиром на то да су модели све бољи у предвиђању податка који недостаје како би попунили празнине у базама података.²⁰⁹

Како би се пронашло решење за уклањање утицаја података на модел ради се на развијању техника одучавања модела (*machine unlearning*). Потпуно одучавање подразумевало би да се модел налази у стању у коме би био да никада није дошао у контакт са одређеним податком, што би тренутно било могуће само путем поновног

²⁰⁴ E. F. Villaronga, P. Kieseberg, T. Li, Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten, *Computer Law & Security Review*, Vol. 34, p. 309.

²⁰⁵ D. Zhang, P. Finckenberg-Broman, T. Hoang, S. Pan, Z. Xing, M. Staples, X. Xu, *op. cit.*, p. 2450.

²⁰⁶ M. Orofino, Il diritto all'oblio alla prova dell'intelligenza artificiale: dal diritto alla de-indicizzazione al diritto al de-addestramento?; in: Orofino M., (ed.), *Chi ha diritto a essere dimenticato? I diritti all'oblio e le sfide contemporanee*, Milano, 2026, p. 48.

²⁰⁷ B. Fernández Delgado, V. Cazorro Barahona, *op. cit.*, p. 7.

²⁰⁸ D. Zhang, P. Finckenberg-Broman, T. Hoang, S. Pan, Z. Xing, M. Staples, X. Xu, *op. cit.*, p. 2450.

²⁰⁹ B. Custers, H. Vrabec, *op. cit.*, p. 10.

тренирања модела.²¹⁰ Важно је имати у виду да су методе попут одучавања углавном тестиране на подацима на енглеском језику, те да још увек није могуће оценити њихову учинковитост на српском и другим језицима.²¹¹

Један од метода одучавања модела је SISA (*Sharded, Isolated, Sliced and Aggregated*). Применом SISA метода скуп тренинг података се дели у „групе“ (*shards*). Када је потребно брисање неког податка о личности, идентификује се којој групи он припада. Податак се брише из ње и модел се поново тренира само у погледу те групе података, док остале групе не подлежу никаквој промени. Овај метод има недостатке у виду смањене тачности модела услед дељења података у групе, као и чињенице да и овакво поновно тренирање модела захтева утрошак времена и средстава.²¹²

Ако би се напустило строго језичко тумачење појма „брисање“ и прибегло циљном тумачењу одредби којима се предвиђа ово право, то може довести до тога да се моделима поставе флексибилнији захтеви усклађености са законом које би они заправо могли да испуне. Право на брисање установљено је са одређеним циљевима заштите права и интереса појединаца који се могу постићи и алтернативним методама. Оне могу укључивати анонимизацију, диференцијалну приватност, као и функционалну енкрипцију.²¹³ Поред наведених, могу се применити и методе попут *Retrieval-Augmented Generation* – RAG, која подразумева да модел приликом закључивања користи податке који се чувају у екстерној бази података, што чини проналажење и брисање података лакшим.²¹⁴ Појам брисања би се могао тумачити и тако да се податак може сматрати избрисаним иако нису избрисане и његове шифроване копије.²¹⁵

Па ипак, постоје ограничења примене ових метода у пракси. Анонимизација се показала као метод који може да доведе до значајних девијација у резултатима алгоритама машинског учења, док функционална енкрипција, која омогућава

²¹⁰ S. Nicolazzo, A. Sapienza, S. Vilella, G. Ruffo, (De-)indicizzazione e diritto all'oblio al tempo dei Large Language Model; in: Orofino M., (ed.), *Chi ha diritto a essere dimenticato? I diritti all'oblio e le sfide contemporanee*, Milano, 2026, p. 94.

²¹¹ A. Blanco-Justicia, J. Domingo-Ferrer, N. M. Jebreel, B. Manzanares-Salor, D. Sánchez, Unlearning in Large Language Models: We Are Not There Yet, *Computer*, Vol. 58(1), p. 99.

²¹² B. A. Juliussen, J. P. Rui, D. Johansen, Algorithms that forget: Machine unlearning and the right to erasure, *Computer Law & Security Review*, Vol. 51, p. 8.

²¹³ E. F. Villaronga, P. Kieseberg, T. Li, *op. cit.*, pp. 310–311.

²¹⁴ S. Nicolazzo, A. Sapienza, S. Vilella, G. Ruffo, *op. cit.*, p. 95.

²¹⁵ European Network and Information Security Agency (ENISA), *The right to be forgotten – between expectations and practice*; преузето 06.10.2026.
<https://www.enisa.europa.eu/sites/default/files/publications/The%20right%20to%20be%20forgotten%20-%20between%20expectations%20and%20practice.pdf>

спровођење математичких операција без потребе декрипције података, није практична за примену на великим базама података на којима се заснивају модели вештачке интелигенције.²¹⁶

Прихватљивост алтернативних метода може се установити и аналогном применом става Суда правде Европске уније приликом формулисања права на заборав, за које је Суд сматрао да би било испуњено уклањањем резултата из листе претраге, иако сам сајт ка коме је резултат претраге водио и даље садржи податак о личности чије се брисање тражи.²¹⁷ OpenAI, на пример, користи појам права на заборав и образлаже га као захтев да се одређени податак не појављује у излазним подацима модела.²¹⁸

Проблем адекватног брисања података би се могао умањити и методама превенције, попут минимизације података²¹⁹ или тренирања модела на анонимизованим подацима. С тим у вези постоје и технике којима се омогућава да се подаци о појединцу прикупљају на начин који искључује могућност његове идентификације, јер су подаци потпуно одвојени у скупу података.²²⁰ Могу се развити и методи којима би се умањио ризик да модел касније генерише податке о личности које је користио приликом учења,²²¹ што може бити олакшано и ако појединци имају могућност да донесу информисану одлуку на самом почетку да прихвате или одбију обраду њихових података.²²²

Превенција олакшава усклађивање са законом. Па ипак, док год постоје подаци о личности чије би се брисање могло захтевати, постоји и потреба налажења адекватног решења за усклађивање права на брисање са обрадом коју врши модел вештачке интелигенције.

Нацрт закона о заштити података о личности у потпуности искључује примену права на брисање код обраде података о личности коришћењем вештачке интелигенције,²²³ али предвиђа да се подаци морају обрисати након испуњења сврхе овакве обраде.²²⁴

²¹⁶ E. F. Villaronga, P. Kieseberg, T. Li, *op. cit.*, p. 310.

²¹⁷ M. Orofino, *op. cit.*, p. 48.

²¹⁸ OpenAI, *op. cit.*

²¹⁹ E. F. Villaronga, P. Kieseberg, T. Li, *op. cit.*, p. 311.

²²⁰ *ibid.*

²²¹ M. Orofino, *op. cit.*, p. 44.

²²² *ibid.*, p. 45.

²²³ Чл. 52. ст. 4. Нацрта закона о заштити података о личности.

²²⁴ Чл. 52. ст. 5. Нацрта закона о заштити података о личности.

VI ПРАВО НА ОГРАНИЧЕЊЕ ОБРАДЕ И ПРИГОВОР

Право на ограничење обраде и приговор на обраду представљају права којима лице на одређени начин може да утиче на то да ли ће се и под којим условима обрада његових података о личности наставити. Између њих постоје и разлике које су изложене у овом поглављу, уз разматрање могућности остваривања ових права у контексту вештачке интелигенције.

1. Право на ограничење обраде

Појединац има право да захтева ограничење обраде у случају незаконите обраде када лице не жели брисање података,²²⁵ као и када руковаоцу више нису потребни подаци за остваривање сврхе обраде, али их лице тражи како би могло да поднесе, оствари или одбрани правни захтев.²²⁶ Ако појединац оспорава тачност податка о личности, руковалац ће на захтев лица ограничити обраду само у року који је потребан за проверу тачности тог податка.²²⁷ Када је појединац претходно уложио приговор на обраду, ограничење обраде се може тражити када се процењује да ли правни, или у случају GDPR-а легитимни основ обраде претеже над интересима лица.²²⁸

Смисао права на ограничење обраде је у томе да руковалац мора да прекине са обрадом података о личности, али их може и даље чувати. Даља обрада је дозвољена и у циљу похрањивања података или подношења, остваривања или одбране правног захтева, као и како би се заштитила права других лица или остварили значајни јавни интереси. За сваку другу даљу обраду је потребан пристанак лица.²²⁹ Руковалац је дужан да обавести лице пре него што ограничење престане да важи.²³⁰

Постоји иста обавеза информисања прималаца података као и код исправке и брисања података. Уколико су подаци подељени са другим субјектима, руковалац је дужан да их информише о ограничењу обраде, сем ако је то немогуће или изискује прекомеран утрошак времена и средстава.²³¹ Лице има право да захтева да буде информисано о тим примаоцима.²³²

²²⁵ Чл. 31. ст. 1. т. 2. ЗЗПЈ; Art. 18(1)(b) GDPR.

²²⁶ Чл. 31. ст. 1. т. 3. ЗЗПЈ; Art. 18(1)(c) GDPR.

²²⁷ Чл. 31. ст. 1. т. 1. ЗЗПЈ; Art. 18(1)(a) GDPR.

²²⁸ Чл. 31. ст. 1. т. 4. ЗЗПЈ; Art. 18(1)(d) GDPR.

²²⁹ Чл. 31. ст. 2. ЗЗПЈ; Art. 18(2) GDPR.

²³⁰ Чл. 31. ст. 3. ЗЗПЈ; Art. 18(3) GDPR.

²³¹ Чл. 33. ст. 1. ЗЗПЈ; Art. 19 GDPR.

²³² Чл. 33. ст. 2. ЗЗПЈ; Art. 19 GDPR.

Начин на који се може спровести ограничење обраде укључује похрањивање података у одвојену базу података, чињење података недоступним корисницима, као и примену одговарајућих техничких мера којима би се осигурало да се подаци даље неће обрађивати и мењати, као и то да је јасно означено да је обрада тих података ограничена.²³³ Код система вештачке интелигенције, оне технологије које омогућавају издвајање података, попут њиховог чувања у бази података која се налази ван структуре модела, могу допринети могућности да се оствари ово право. Потребно је да модел буде у стању да доследно прати инструкције да податак не користи у одређеном временском периоду ни у какве сврхе.

Нацрт закона о заштити података о личности у потпуности искључује могућност ограничења обраде када се она врши коришћењем вештачке интелигенције.²³⁴

2. Право на приговор

Право на приговор је правно средство доступно појединцу против обраде података о личности.²³⁵ Међутим, оно није доступно у свим случајевима обраде. Ако лице сматра да је то оправдано узимајући у обзир његову посебну ситуацију, приговор се може уложити руковоацу када је правни основ обраде легитимни интерес, као и када је обрада неопходна за обављање послова у јавном интересу или извршење законских овлашћења руковоаца.²³⁶

Независно од правног основа обраде, уколико се она врши у сврхе директног оглашавања, појединац има безусловно право да уложи приговор на такву обраду, као и на профилисање у те сврхе. С обзиром на то да је у овом случају приговор везан за сврху обраде, подаци о личности на које се приговор односи се даље могу обрађивати у друге сврхе које нису директно оглашавање.²³⁷ Закон прописује и право на приговор уколико се подаци обрађују у сврхе научног или историјског истраживања или статистичке сврхе, али прописује и да се право у том случају неће примењивати уколико је обрада неопходна за обављање послова у јавном интересу.²³⁸

²³³ Recital 67 GDPR.

²³⁴ Чл. 52. ст. 4. Нацрта закона о заштити података о личности.

²³⁵ С. Андоновић, Д. Прља, *op. cit.*, стр. 114.

²³⁶ Чл. 37. ст. 1. ЗЗПЈ; Art. 21(1) GDPR.

²³⁷ Чл. 37. ст. 2. ЗЗПЈ; Art. 21(2) GDPR.

²³⁸ Чл. 37. ст. 6. ЗЗПЈ; Art. 21(6) GDPR.

Руковалац је на основу приговора дужан да прекине са обрадом. Обрада се може наставити само ако руковалац предочи да за њу постоје законски разлози који претежу над интересима лица или су везани за подношење, остваривање или одбрану правног захтева.²³⁹ Anthropic, на пример, наводи да ће и поред приговора појединца користити улазне и излазне податке за унапређење модела ако су разговори са тим корисником пријављени као небезбедни, наводећи потребу да се побољша механизам откривања штетног садржаја, примене политике руковаоца или развија истраживање безбедности вештачке интелигенције, или ако је корисник изричито пријавио материјал са подацима о личности путем, на пример, механизма којим корисници дају повратне информације.²⁴⁰

Уочљива је разлика у томе како је ово право формулисано у GDPR-у, који тражи од руковаоца да предочи „уверљиве легитимне основе“ за обраду уместо „законских разлога“ предвиђених ЗЗПЈ-ом. То не значи нужно да је законодавац имао намеру да захтева да разлози за настављање обраде буду изричито прописани законом, али је потребно јасно тумачење како би се отклонила свака недоумица.

Када се руковаоци ослањају на легитимни интерес као правни основ обраде података коришћењем модела вештачке интелигенције, потребно је узети у обзир чињеницу да ће се у том случају примењивати право на приговор.²⁴¹ Најкасније при првој комуникацији са руковаоцем, појединац мора бити изричито и одвојено од свих других информација обавештен о свом праву на приговор.²⁴² Лице има право и да приговор поднесе аутоматизованим путем, на начин на који је то технички изводљиво, уколико се подаци обрађују приликом коришћења услуга информационог друштва.²⁴³

У пракси руковаоци могу да омогуће корисницима да уложе приговор на обраду података које модел прикупља из њихових упита у виду јасно доступне *opt-out* опције.²⁴⁴ Руковаоци углавном и посежу за оваквим решењем, те се упити аутоматски обрађују за сврхе тренирања модела, али се појединцима пружа опција да искључе могућност такве обраде. *Opt-out* механизам се може пружити и пре почетка тренирања модела и тако

²³⁹ Чл. 37. ст. 1. ЗЗПЈ; Art. 21(1) GDPR.

²⁴⁰ Anthropic, *Privacy Policy*, *op. cit.*

²⁴¹ European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, *op. cit.*

²⁴² Чл. 37. ст. 4. ЗЗПЈ; Art. 21(4) GDPR.

²⁴³ Чл. 37. ст. 5. ЗЗПЈ; Art. 21(5) GDPR.

²⁴⁴ Т. Н. Тасић, *Балансирање између иновација и заштите података о личности на примеру ChatGPT-a*, *Страни правни живот*, Vol. 70(1), стр. 33.

омогућити појединцу да приговори и на обраду података за учење модела. Meta је, на пример, била у обавези да омогући појединцима да уложи приговор на обраду својих јавно доступних података на платформи пре него што крене са тренирањем модела.²⁴⁵

Нацрт закона о заштити података о личности ово право ограничава на исти начин као и право на приступ подацима уколико се они обрађују коришћењем вештачке интелигенције.²⁴⁶

²⁴⁵ Data Protection Commission, *DPC Statement on Meta AI*; преузето 06.10.2026.
<https://www.dataprotection.ie/en/news-media/latest-news/dpc-statement-meta-ai>

²⁴⁶ Чл. 52. ст. 3. Нацрта закона о заштити података о личности.

VII DAЉI RAZVOJ PRAVA LIЦА ЧИЈИ СЕ ПОДАЦИ О ЛИЧНОСТИ ОБРАЂУЈУ ОД СТРАНЕ МОДЕЛА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ

Република Србија још увек нема засебан закон који регулише вештачку интелигенцију, али је његово усвајање предвиђено Стратегијом развоја вештачке интелигенције за период 2025–2030. године.²⁴⁷ Са друге стране, законодавство Европске уније даље напредује у тежњи да се постигне већи баланс између супротстављених интереса компанија и појединаца. Тренутно се разматра Дигитални омнибус (*Digital Omnibus*),²⁴⁸ документ који има за циљ да олакша примену и хармонизацију законодавства које уређује дигитални свет, укључујући и GDPR. Одређене измене Уредбе ЕУ о вештачкој интелигенцији уведене су Дигиталним омнибусом о вештачкој интелигенцији,²⁴⁹ који је као део Дигиталног омнибуса ступио на снагу јула 2026. године.²⁵⁰ Остатак Дигиталног омнибуса још увек није усвојен.

Када је у питању Нацрт закона о заштити података о личности Републике Србије, потребно је узети у обзир да Уредба ЕУ о вештачкој интелигенцији прокламује да се правила заштите података о личности и даље примењују уз све обавезе предвиђене Уредбом.²⁵¹ Вреди напоменути и да се као измена GDPR-а у оквиру Дигиталног омнибуса предлаже увођење безусловног права на приговор на обраду података о личности ради развоја система вештачке интелигенције.²⁵² То води закључку да Европска унија сматра да је потребно да стандарди заштите података о личности буду технолошки неутрални, те да обрада од стране вештачке интелигенције не сме дерогирати, између осталог, права лица на која се подаци односе. Имајући то у виду, нејасна је намера законодавца у Републици Србији и смер у коме се жели развој права, с обзиром на то да Нацрт закона о заштити података о личности изричито искључује примену одређених права када се подаци о личности обрађују коришћењем вештачке интелигенције. Предложена решења

²⁴⁷ Стратегија развоја вештачке интелигенције у Републици Србији за период 2025–2030. година, *Службени гласник РС*, бр. 5/2025-10.

²⁴⁸ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus).

²⁴⁹ Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI).

²⁵⁰ European Commission, *AI Omnibus enters into force*; преузето 15.08.2026. <https://digital-strategy.ec.europa.eu/en/news/ai-omnibus-enters-force>

²⁵¹ Art. 2(7) EU AI Act.

²⁵² Art. 88c GDPR (у тексту предложеном Дигиталним омнибусом).

могу изазвати више проблема и недоумица које је потребно разматрати и отклонити пре усвајања Нацрта закона.

Најпре, потребно је да појам „вештачке интелигенције“ буде прецизно дефинисан у закону који ће у Републици Србији регулисати вештачку интелигенцију, као што то чини Уредба ЕУ о вештачкој интелигенцији. Ако се у усвоје одредбе Нацрта закона којима се онемогућава остваривање права, неопходно је да буде одређено ван сваке сумње који случајеви обраде ће довести до тога.

Затим, када се подаци који се користе за развој модела не прикупљају непосредно од лица на које се односе, идентификација тог лица може бити отежана за руковооца, те се може јавити злоупотреба изузетака од примене права на приступ и приговор који се предлажу у Нацрту. Meta, на пример, пружа обавештење појединцима у коме тврди да се подаци о личности прикупљени од трећих страна за развој Meta модела вештачке интелигенције не повезују са конкретним Meta налогом, нити се чувају на начин који разумно омогућава идентификацију особе. Самим тим, наглашава да не пружа могућност остваривања права приступа, преносивости, исправке или допуне, нити брисања тих података.²⁵³ Anthropic за свој Claude систем овај проблем формулише у виду тога да се у случају да се појединац не може идентификовати могу јавити ограничења приликом одговарања на захтев лица у вези са његовим правима.²⁵⁴ Стога је од изузетне важности прецизно поставити сваки изузетак који онемогућава лице да остварује своја права. Поред тога, потребно је да буде јасно када би остваривање сврхе обраде било значајно отежано, као и то да је терет доказивања на руковооцу.

Даље, потпуно искључивање примене права на исправку и допуну, ограничење обраде, брисање и преносивост података када се подаци обрађују коришћењем вештачке интелигенције представљало би велики корак назад за заштиту података о личности у Републици Србији. У атмосфери у којој се говори о обезбеђивању што веће заштите појединаца, Нацрт закона би на овај начин ефективно одузео појединцима контролу над њиховим подацима у све заступљенијој технологији обраде, чије се негативне последице на права лица тренутно највише и истичу. Ни сами руковооци у пракси не ограничавају права лица у оној мери у којој то чини Нацрт закона, макар када су њихови корисници у

²⁵³ Facebook, *Data Subject Rights for Third Party Information Used for AI at Meta*; преузето 06.10.2026.
<https://www.facebook.com/help/contact/510058597920541>

²⁵⁴ Anthropic, *Privacy rights requests relating to Anthropic's training data*; преузето 06.10.2026.
<https://privacy.claude.com/en/articles/15865314-privacy-rights-requests-relating-to-anthropic-s-training-data>

питању. Уз то, нејасан је домен ограничења права у вези са аутоматизованим доношењем појединачних одлука. Потребно је прецизирати одредбе којима се забрањује и дозвољава обрада искључиво системом вештачке интелигенције, као и повезати их са аутоматизованим доношењем одлука ако је то могуће.

Нацрт закона свакако уводи и решења којима се побољшава положај појединца. Решење којим се налаже руковоцу да информише лице о категоријама података које обрађује чак и када је податке прикупио непосредно од њега одговара најбољој пракси која омогућава адекватну информисаност појединаца. Све чешће се подаци прикупљају непосредно од лица на које се односе без њиховог знања. На пример, информације о понашању и интересовањима појединаца прикупљају се њиховим посматрањем или праћењем. Иако такве информације појединац није свесно дао руковоцу, оне се и даље могу сматрати непосредно прикупљеним од тог лица. Самим тим, важно је да су појединци информисани о томе које се све информације које су свесно или несвесно дали руковоцу обрађују, како би могли да остварују своја права у односу на такву обраду. Свакако, руковалац према тренутним законским решењима није спречен да пружи и додатне информације, те је добра пракса да увек информише лице и о категоријама података које се прикупљају и обрађују.

ЗАКЉУЧАК

Почетна фаза убрзаног развоја технологије вештачке интелигенције представљала је плодно тло за иновације без нарочитих ограничења. Потенцијални ризици технологије су били занемарени све док нису кренули да се материјализују. Када је коначно започета дискусија о примени тренутно постојећих законских оквира и усвајању нових, законодавци су кренули да постављају границе иновација тамо где их до сада није било. Тада је настао проблем усаглашавања већ развијених модела вештачке интелигенције са законом, а добављачи који сада развијају моделе су под већим притиском да модел буде у могућности да испуњава све захтеве закона у односу на раније.

Закључци до којих доводи истраживање изложено у овом раду свODE се на то да је потребно двојако прилагођавање како би појединци могли ефективно да остварују своја права. Са једне стране, потребно је прилагођавање постојећих законских одредби и увођење нових, уз максималну технолошку неутралност како би могли да буду применљиви што дуже. Са друге стране, потребне су измене у начину рада модела како би се омогућило испуњење законских обавеза. Моделе вештачке интелигенције би требало развијати пре свега имајући у виду начело заштите података о личности према коме заштита и минимизација података мора бити у сржи начина на који функционише систем који обрађује податке о личности (*privacy by design*).²⁵⁵ С тим у вези актуелно је развијање технолошких решења која омогућавају већу заштиту података о личности (*privacy enhancing technologies*). Постоји потреба да се технологија и начин на који функционишу базе података које представљају основу модела вештачке интелигенције пројектују тако да истовремено омогуће ефикасност модела и дозволе испуњавање захтева закона о заштити података,²⁵⁶ као и да се у сам модел уграде одговарајуће мере које ће обезбедити адекватну заштиту појединаца.

Задаци које ће модели научити да раде и начин на који ће их радити зависе од процеса учења и информација које им се притом дају. Како би се одређене вредности и начела усадили у начин на који модел функционише, компаније које развијају моделе вештачке интелигенције усвајају документе који садрже те вредности. Модел затим тренирају на тим документима како би се он водио тим принципима у свом раду. На пример, компанија Microsoft усвојила је, између осталог, Кодекс понашања, који је ставила на

²⁵⁵ Чл. 42. ЗЗПЈ; Art. 25 GDPR.

²⁵⁶ E. F. Villaronga, P. Kieseberg, T. Li, *op. cit.*, p. 311.

увид јавности пре него што крене да тренира своје моделе на њему. Овај документ садржи и принципе важне за усклађивање обраде података о личности коју ће модел вршити са захтевима закона. Ту спадају упутства моделу да избегава да приступа подацима који му нису неопходни за извршење неког задатка, како би се испунило начело минимизације података, затим процес размишљања и принципи којима ће се модел водити пре него што обради одређен податак о личности, као и начело према коме је потребно одржати људску контролу над моделом.²⁵⁷ Anthropic је такође усвојио овакав тип документа и назвао га Уставом.²⁵⁸ Без обзира на назив за који се добављач определи, овакви документи су један од начина на који се усаглашавање са законом и заштита права појединаца може уградити у само понашање и начин размишљања модела.

Појединци нису у довољној мери свесни својих права због тога што не читају документацију, нити могу у потпуности да је разумеју. Самим тим, потребно је и прилагођавање начина на који се информације пружају. Једна од опција може бити да модел пружа информације појединцу. Ово би могло бити корисно због тога што је моделу лако да прилагоди начин и темпо којим ће објаснити обраду, како не би преоптеретио појединца. Модел може да врши прилагођавање и на основу претпостављеног нивоа стручности појединца на основу онога што он зна о њему,²⁵⁹ уколико је, наравно, таква обрада законита. Важно је у овом случају да је модел претходно адекватно истрениран да увек пружи тачне и потпуне информације, као и референцу ка документу који их подупире. Свакако, овако пружено обавештење може бити само допуна обавештења које даје руковалац, и не сме га у потпуности заменити услед тога што модел може давати и нетачне податке у виду халуцинација.

С обзиром на то да се људи све више ослањају на вештачку интелигенцију као извор информација, халуцинације доприносе општем проблему ширења дезинформација, али су оне нарочито проблематичне када укључују податке о личности. Халуцинације између осталог могу негативно утицати и на одлуке које се доносе аутоматизованом обрадом, јер се одлука која има значајан утицај на појединца тада може заснивати на нетачним подацима. Такође, треба имати у виду да подаци у виду халуцинација сами по себи нису део скупа података за учење модела, те их је јако тешко уклонити.²⁶⁰ Проблем

²⁵⁷ Microsoft AI, *Humanist AI Code of Conduct*; преузето 29.09.2026. <https://microsoft.ai/code-of-conduct/>

²⁵⁸ Anthropic, *Claude's Constitution*; преузето 07.10.2026. <https://www.anthropic.com/constitution>

²⁵⁹ R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, D. Pedreschi, A survey of methods for explaining black box models, *ACM computing surveys (CSUR)*, Vol. 51(5), p. 6.

²⁶⁰ D. Zhang, P. Finckenberg-Broman, T. Hoang, S. Pan, Z. Xing, M. Staples, X. Xu, *op. cit.*, p. 2450.

халуцинација је потребно даље разматрати и идентификовати потенцијална законска и технолошка решења којим би се умањио његов негативан утицај на права појединаца.

Поред тога, важно је истаћи и да треба бити обазрив када се подаци карактеришу као анонимизовани подаци. Модели су већ сада способни да потенцијално пониште анонимизацију и податак повежу са другим податком који би омогућио идентификацију лица.²⁶¹ Због тога је важно да надзорна тела и законодавци наставе да развијају стандарде анонимизације који су ефективни у пракси, као и да их руковооци примењују и пажљиво процењују да ли подаци испуњавају све прописане услове да буду анонимизовани, узимајући у обзир све предузете мере.

На крају, може се изнети аргумент да ће системи вештачке интелигенције у будућности бити све комплекснији, те да ће бити још теже испунити захтеве транспарентности и осталих права лица на која се подаци односе.²⁶² Међутим, управо је то разлог због кога је потребно радити на томе да се поставе границе и стандарди у развоју система вештачке интелигенције који морају бити испуњени како би модел могао да омогући остваривање права у складу са законом. Нема разлога да један од праваца којим би се могао кретати напредак ове технологије не буде онај у коме се приоритизују права појединаца.

²⁶¹ Ђ. Кривокапић, А. Николић, Регулисање вештачке интелигенције – стање и перспективе, *Ревуја копаоничке школе природног права*, Vol. 1/2022, стр. 103.

²⁶² Y. Bathaee, The Artificial Intelligence Black Box and the Failure of Intent and Causation, *Harvard Journal of Law & Technology*, Vol. 31(2), p. 929.

ПОПИС КОРИШЋЕНЕ ЛИТЕРАТУРЕ

1. Агенција Европске уније за основна права и Савет Европе, *Приручник о европском праву заштите података*; преузето 11.08.2026. <https://poverenik.rs/h-content/uploads/2024/03/HF42-prirucnik-evropsko-pravo-zastite-podataka-SRP-poverenik.pdf>;
2. Андоновић Стефан, Прља Драган, *Основи права заштите података о личности*, Београд, 2020, Институт за упоредно право;
3. Anthropic, *Claude's Constitution*; преузето 07.10.2026. <https://www.anthropic.com/constitution>;
4. Anthropic, *Privacy Policy*; преузето 06.10.2026. <https://www.anthropic.com/legal/privacy>;
5. Anthropic, *Privacy rights requests relating to Anthropic's training data*; преузето 06.10.2026. <https://privacy.claude.com/en/articles/15865314-privacy-rights-requests-relating-to-anthropic-s-training-data>;
6. Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*; преузето 14.09.2026. <https://ec.europa.eu/newsroom/article29/items/612053>;
7. Article 29 Data Protection Working Party, *Guidelines on the right to data portability*; преузето 06.10.2026. <https://ec.europa.eu/newsroom/article29/items/611233>;
8. Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679*; преузето 16.08.2026. https://www.edpb.europa.eu/documents/guideline/article-29-working-party-guidelines-on-transparency-under-regulation-2016679_en;
9. Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*; преузето 29.09.2026. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf;
10. Bathaee Yavar, The Artificial Intelligence Black Box and the Failure of Intent and Causation, *Harvard Journal of Law & Technology*, Vol. 31(2), pp. 889–938;
11. Blanco-Justicia Alberto, Domingo-Ferrer Josep, Jebreel Najeeb Moharram, Manzanares-Salor Benet, Sánchez David, Unlearning in Large Language Models: We Are Not There Yet, *Computer*, Vol. 58(1), pp. 97–100;
12. Bordt Sebastian, Finck Michèle, Raidl Eric, von Luxburg Ulrike, Post-Hoc Explanations Fail to Achieve Their Purpose in Adversarial Contexts; in: *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, Seoul, 2022, Association for Computing Machinery, pp. 891–905;
13. Castellanos Claramunt Jorge, La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos, *Métodos de Información*, Vol. 11(21), pp. 59–82;
14. Commission Nationale de l'Informatique et des Libertés (CNIL), *IA: Informer les personnes concernées*; преузето 12.07.2026. <https://www.cnil.fr/fr/ia-informer-les-personnes-concernees>;

15. Custers Bart, Vrabec Helena, Tell me something new: data subject rights applied to inferred data and profiles, *Computer Law & Security Review*, Vol. 52, Article no. 105956;
16. Data Protection Commission, *DPC Statement on Meta AI*; преузето 06.10.2026. <https://www.dataprotection.ie/en/news-media/latest-news/dpc-statement-meta-ai>;
17. Дилигенски Андреј, Прља Драган, Церовић Дражен, *Право заштите података GDPR*, Београд, 2018, Институт за упоредно право;
18. Edwards Lillian, Veale Michael, Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”?, *IEEE Security & Privacy*, Vol. 16(3), pp. 46–54;
19. European Commission, *AI Omnibus enters into force*; преузето 15.08.2026. <https://digital-strategy.ec.europa.eu/en/news/ai-omnibus-enters-force>;
20. European Data Protection Board, *Guidelines 03/2026 on web scraping in the context of generative AI*; преузето 13.08.2026. https://www.edpb.europa.eu/public-consultations/guidelines-032026-on-web-scraping-in-the-context-of-generative-ai_en#no-back;
21. European Data Protection Board, *Guidelines 02/2026 on Anonymisation*; преузето 29.09.2026. https://www.edpb.europa.eu/public-consultations/guidelines-022026-on-anonymisation_en;
22. European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*; преузето 04.10.2026. https://www.edpb.europa.eu/system/files/documents/2024-12/edpb_opinion_202428_ai-models_en.pdf;
23. European Data Protection Board, *Guidelines 01/2022 on data subject rights - Right of access*; преузето 03.10.2026. https://www.edpb.europa.eu/system/files/documents/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf;
24. European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*; преузето 26.09.2026. https://www.edpb.europa.eu/documents/guideline/guidelines-072020-on-the-concepts-of-controller-and-processor-in-the-gdpr_en;
25. European Data Protection Supervisor, *TechDispatch #2/2023 - Explainable Artificial Intelligence*; преузето 17.08.2026. https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-22023-explainable-artificial-intelligence_en;
26. European Network and Information Security Agency (ENISA), *The right to be forgotten – between expectations and practice*; преузето 06.10.2026. <https://www.enisa.europa.eu/sites/default/files/publications/The%20right%20to%20be%20forgotten%20-%20between%20expectations%20and%20practice.pdf>;
27. European Parliament: Directorate-General for Parliamentary Research Services, *The impact of the general data protection regulation on artificial intelligence*, 2020, Publications Office;
28. Facebook, *Data Subject Rights for Third Party Information Used for AI at Meta*; преузето 06.10.2026. <https://www.facebook.com/help/contact/510058597920541>;

29. Felzmann Heike, Villaronga Eduard Fosch, Lutz Christoph, Tamò-Larrieux Aurelia, Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns, *Big Data & Society*, Vol. 6(1), pp. 1–14;
30. Fernández Delgado Beatriz, Cazurro Barahona Víctor, Can artificial intelligence forget? Reflections on the right to disappear in a world where algorithms remember everything, *International Journal of Engineering Business Management*, Vol. 18, pp. 1–12;
31. Guidotti Riccardo, Monreale Anna, Ruggieri Salvatore, Turini Franco, Giannotti Fosca, Pedreschi Dino, A survey of methods for explaining black box models, *ACM computing surveys (CSUR)*, Vol. 51(5), pp. 1–42;
32. Häuselmann Andreas, Custers Bart, The Right to Rectification and Inferred Personal Data, *European Journal of Law and Technology*, Vol. 15 (3);
33. Hawkins Katie, Alhuwaish Nora, Belguith Sana, Vranaki Asma, Charlesworth Andrew, A Decision-Making Process to Implement the ‘Right to Be Forgotten’ in Machine Learning; in: Rannenber Kai, Droghkaris Prokopios and Lauradoux Cédric, (eds.), *Privacy Technologies and Policy - APF 2023, Lyon, France, June 1–2, 2023, Proceedings*, Cham, 2024, Springer Science and Business Media Deutschland GmbH, pp. 20–38;
34. Humerick Matthew, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *Santa Clara High Technology Law Journal*, Vol. 34(4), pp. 393–418;
35. Juliussen Bjørn Aslak, Rui Jon Petter, Johansen Dag, Algorithms that forget: Machine unlearning and the right to erasure, *Computer Law & Security Review*, Vol. 51, Article no. 105885;
36. Kaminski Margot E., Urban Jennifer M., The Right to Contest AI, *Columbia Law Review*, Vol. 121(7), pp. 1957–2048;
37. Кривокапић Ђорђе, Николић Андреа, Регулисање вештачке интелигенције – стање и перспективе, *Ревуја копаоничке школе природног права*, Vol. 1/2022, стр. 93–111;
38. Microsoft AI, *Humanist AI Code of Conduct*; преузето 29.09.2026. <https://microsoft.ai/code-of-conduct/>;
39. Mistral, *AI Governance*; преузето 07.10.2026. <https://legal.mistral.ai/>;
40. Naghiyev Kanan, ChatGPT From a Data Protection Perspective, *Baku State University Law Review*, Vol. 10(1), pp. 1–34;
41. Nicolazzo Serena, Sapienza Anna, Vilella Salvatore, Ruffo Giancarlo, (De-)indicizzazione e diritto all’oblio al tempo dei Large Language Model; in: Orofino Marco, (ed.), *Chi ha diritto a essere dimenticato? I diritti all’oblio e le sfide contemporanee*, Milano, 2026, Milano University Press, pp. 77–99;
42. OpenAI, *Right to be forgotten and personal data removal from ChatGPT*; преузето 06.10.2026. <https://help.openai.com/en/articles/20001057-right-to-be-forgotten-and-personal-data-removal-from-chatgpt>;
43. Orofino Marco, Il diritto all’oblio alla prova dell’intelligenza artificiale: dal diritto alla de-indicizzazione al diritto al de-addestramento?; in: Orofino Marco, (ed.), *Chi ha diritto a essere dimenticato? I diritti all’oblio e le sfide contemporanee*, Milano, 2026, Milano University Press, pp. 27–49;

44. Повереник за информације од јавног значаја и заштиту података о личности, *Заштита података о личности: Ставови, мишљења и пракса Повереника, Публикација бр. 10*, Београд, 2025;
45. Повереник за информације од јавног значаја и заштиту података о личности, *Заштита података о личности: Ставови и мишљења Повереника, Публикација бр. 6*, Београд, 2021;
46. Прља Драган, Гасми Гордана, Кораћ Вања, *Вештачка интелигенција у правном систему ЕУ*, Београд, 2021, Институт за упоредно право;
47. Silva Gomes Rute, Data subject rights in the era of AI. Can the right of rectification protect data subjects against incorrect inferences made by artificial intelligence systems?, *Quaderns IEE: Revista de l'Institut d'Estudis Europeus*, Vol. 4(2), pp. 85–111;
48. SpaceXAI, *SpaceXAI's Europe Privacy Policy Addendum*; преузето 06.10.2026. <https://x.ai/legal/europe-privacy-policy-addendum>;
49. Stanford Institute for Human Centered Artificial Intelligence, Center for Research on Foundation Models – CRFM, *The 2025 Foundation Model Transparency Index*; преузето 12.08.2026. <https://crfm.stanford.edu/fmti/December-2025/paper.pdf>;
50. Тасић Тамара Н., Балансирање између иновација и заштите података о личности на примеру ChatGPT-а, *Страни правни живот*, Vol. 70(1), стр. 21–38;
51. The European Commission's High-Level Expert Group on Artificial Intelligence, *A Definition of AI: Main Capabilities and Scientific Disciplines*; преузето 23.09.2026. https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf;
52. Villaronga Eduard Fosch, Kieseberg Peter, Li Tiffany, Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten, *Computer Law & Security Review*, Vol. 34, pp. 304–313;
53. Wachter Sandra, Mittelstadt Brent, Floridi Luciano, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, Vol. 7(2), pp. 76–99;
54. Wachter Sandra, Mittelstadt Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, *Columbia Business Law Review*, Vol. 2019(2), pp. 494–620;
55. Zarsky Tal Z., Incompatible: The GDPR in the Age of Big Data, *Seton Hall Law Review*, Vol. 47, pp. 995–1020;
56. Zhang Dawen, Finckenberg-Broman Pamela, Hoang Thong, Pan Shidong, Xing Zhenchang, Staples Mark, Xu Xiwei, Right to Be Forgotten in the Era of Large Language Models: Implications, Challenges, and Solutions, *AI and Ethics*, Vol. 5(3), pp. 2445–2454;

ПОПИС ОСТАЛЕ ИСТРАЖИВАЧКЕ ГРАЋЕ

1. Cal. Assemb. Bill No. 2013, 2023-2024 Reg. Sess., ch. 817;
2. Case C-460/20, *Google (Déréférencement d'un contenu prétendument inexact)*, Judgment of 8 December 2022, ECLI:EU:C:2022:962;
3. Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Judgment of 13 May 2014, ECLI:EU:C:2014:317;
4. Case C-413/23 P, *European Data Protection Supervisor (EDPS) v Single Resolution Board (SRB)*, Judgment of 4 September 2025, ECLI:EU:C:2025:645;
5. Case C-252/21, *Meta v Bundeskartellamt*, Judgment of 4 July 2023, ECLI:EU:C:2023:537;
6. Case C-634/21, *OQ v Land Hessen, interveners: SCHUFA Holding AG (SCHUFA Holding and Others)*, Judgement of 7 December 2023, ECLI:EU:C:2023:957;
7. Case C-434/16, *Peter Nowak v Data Protection Commissioner*, Judgment of 20 December 2017, ECLI:EU:C:2017:994;
8. 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;
9. Garante per la protezione dei dati personali, *Provvedimento dell'11 aprile 2023 [9874702]*; преузето 14.07.2026.
<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702>;
10. Министарство правде, Нацрт закона о заштити података о личности; преузето 11.08.2026. <https://mpravde.gov.rs/javne-rasprave>;
11. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus);
12. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI);
13. 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);
14. 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);

15. Стратегија развоја вештачке интелигенције у Републици Србији за период 2025–2030. година, *Службени гласник РС*, бр. 5/2025-10.
16. Закључак о усвајању Етичких смерница за развој, примену и употребу поуздане и одговорне вештачке интелигенције, *Службени гласник РС*, бр. 23/2023-19;
17. Закон о заштити података о личности, *Службени гласник РС*, бр. 87/2018-54;

САЖЕТАК

Рад истражује у којој мери је могуће остварити права која појединци имају у вези са својим подацима о личности које обрађује модел вештачке интелигенције. Настоји да идентификује правне празнине у постојећем законском оквиру и да укаже на постојећа и могућа законска и технолошка решења којима би се отклониле сметње у остваривању права. Истраживање је спроведено применом нормативног, догматског и упоредног метода, као и метода анализе садржаја и анализе случаја. Законски оквир представљају прописи Републике Србије и Европске уније. Рад се осврће и на стручну литературу, мишљења и смернице надзорних тела, праксу Суда правде Европске уније, као и тренутну праксу компанија које развијају моделе вештачке интелигенције.

Уз излагање законског оквира који се разматра у раду, истакнуте су особине технологије вештачке интелигенције које могу утицати на заштиту података о личности. Централни део рада посвећен је садржају, начину остваривања и изузецима од примене права на информисаност, приступ, исправку и допуну, брисање, ограничење обраде, преносивост и приговор, као и права у вези са аутоматизованим доношењем одлука и профилисањем. Рад испитује и додатне улоге и обавезе које се уводе Уредбом Европске уније о вештачкој интелигенцији.

Резултати истраживања показују да су постојећи прописи начелно применљиви на обраду података о личности коју врши вештачка интелигенција, али и да у том случају остваривање појединих права у пракси може бити отежано на одређен начин. Поставља се питање у којој мери права лица на која се подаци односе обухватају изведене податке које је модел вештачке интелигенције створио на основу других података. Потпуно брисање података је технички захтевно, а технике одучавања модела још увек нису довољно развијене. Ограничена објашњивост модела отежава пружање сврсисходних информација о логици аутоматизованог одлучивања. Поред тога, руковоци нису довољно транспарентни и често се ослањају на изузетке од обавезе непосредног информисања лица.

Рад посебно указује и на предлоге одредби у Нацрту закона о заштити података о личности Републике Србије којима се ограничавају или у потпуности искључују права појединаца када се подаци обрађују коришћењем вештачке интелигенције, што није усклађено са правцем у коме се развија легислатива Европске уније. Тиме се разматра

развој права заштите података о личности у односу на технологију вештачке интелигенције.

Закључује се да је за ефективно остваривање права потребно двојако прилагођавање. Са једне стране, потребно је постојеће прописе протумачити на начин који би омогућио да буду што је више могуће применљиви на обраду коју врши вештачка интелигенција, као и да нови прописи који се усвајају буду технолошки неутрални. Са друге стране, модели вештачке интелигенције би требало да се пројектују и развијају тако да се у што већој мери омогући остваривање права и да заштита података о личности од самог почетка буде њихов саставни део.

Кључне речи: вештачка интелигенција, заштита података о личности, права лица на која се подаци односе, изведени подаци, Закон о заштити података о личности, GDPR

ABSTRACT

“Rights of Data Subjects Whose Personal Data Are Processed by Artificial Intelligence Models”

This thesis explores the extent to which data subjects can exercise the rights they have regarding their personal data processed by artificial intelligence models. It seeks to identify legal gaps in the existing regulatory framework and to highlight current and possible legal and technological solutions that could remove obstacles to the exercise of these rights. The research employs normative, dogmatic, and comparative methods, as well as content analysis and case studies. The legal framework encompasses legislation of the Republic of Serbia and the European Union. The thesis also draws upon academic literature, opinions and guidelines from supervisory authorities, the case law of the Court of Justice of the European Union, and the current practices of companies developing artificial intelligence models.

Alongside an overview of the relevant legal framework, the thesis highlights characteristics of artificial intelligence technology that may impact personal data protection. The core section of the thesis addresses the content and exercise of, and exceptions to, the rights to information, access, rectification, erasure, restriction of processing, data portability and objection, as well as the rights related to automated decision-making and profiling. Furthermore, the thesis examines additional roles and obligations introduced by the European Union's Artificial Intelligence Act.

The findings of this research indicate that existing legislation can generally be applied to the processing of personal data by artificial intelligence, but the practical exercise of certain rights may be hindered in some ways. A question arises regarding the extent to which the rights of data subjects extend to inferred data generated by an AI model on the basis of other data. Complete data deletion is technically challenging and machine unlearning techniques are not yet sufficiently developed. The limited explainability of models complicates the provision of meaningful information regarding the logic of automated decision-making. Furthermore, controllers are not sufficiently transparent and frequently rely on exceptions to the obligation to provide information directly to data subjects.

The thesis particularly highlights the proposed provisions of the Draft Law on Personal Data Protection of the Republic of Serbia that restrict or entirely exclude data subject rights in relation to artificial intelligence, an approach inconsistent with the direction in which the European Union's legislative development is heading. In doing so, the thesis examines how data protection is developing in the context of artificial intelligence technology.

The thesis concludes that the effective exercise of rights requires a twofold adjustment. On the one hand, existing legislation must be interpreted in a manner that enables its applicability to AI-driven data processing, while newly adopted legal provisions should be technologically neutral. On the other hand, artificial intelligence models should be designed and developed in a way that maximizes the possibility of exercising rights and ensures that data protection is an integral part of the model from the very outset.

Keywords: artificial intelligence, personal data protection, data subject rights, inferred data, Law on Personal Data Protection, GDPR

БИОГРАФИЈА СТУДЕНТА

Ленка Секулић је рођена 27. децембра 2001. године у Нишу. Основну и средњу школу завршила је као носилац Вукове дипломе. Похађала је билингвално одељење за енглески језик гимназије „Светозар Марковић“ у Нишу. Правни факултет у Нишу је уписала 2020. године и завршила основне академске студије права октобра 2024. године са просеком 9,07. Исте године уписала је мастер академске студије права, смер право и информационе технологије.

Каријеру у области заштите података о личности започела је 2024. године. Као консултант претежно ради са иностраним клијентима, те познаје законодавство у овој области у више различитих правних система. Носи звање сертифициваног стручњака за приватност за Европску унију (*Certified Information Privacy Professional/Europe – CIPP/E*) и чланица је Међународног удружења стручњака за приватност (*International Association of Privacy Professionals – IAPP*), а интересовања су јој усмерена и ка правном регулисању вештачке интелигенције.

Течно говори енглески, а познаје и италијански, француски, шпански и немачки језик. Њене студије обележиле су разне ваннаставне активности. Тимови чији је била члан освојили су треће место на такмичењу у симулацији поступка пред Европским судом за људска права „Бранко Маринковић“, као и прво место на такмичењу „Осуди дискриминацију“ Повереника за заштиту равноправности, на коме је њен тим освојио неколико награда, укључујући и награду за најбољи писани поднесак. Похађала је предавања, обуке и клинике на којима је стекла разна правничка знања и вештине. Била је члан неколико студентских организација, у којима је радила на организацији међународних и локалних пројеката, предавања, конференција и многих других активности.

**ИЗЈАВА О ИСТОВЕТНОСТИ
ШТАМПАНОГ И ЕЛЕКТРОНСКОГ ОБЛИКА МАСТЕР РАДА**

Име и презиме аутора мастер рада: Ленка Секулић

Наслов мастер рада: Права лица чији се подаци о личности обрађују од стране
модела вештачке интелигенције

Коментори: Проф. др Дејан Вучетић и др Велимир Илић

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

У Нишу, _____

Потпис аутора

ИЗЈАВА О АУТОРСТВУ И ОДОБРАВАЊУ ОБЈАВЉИВАЊА МАСТЕР РАДА

Изјављујем да је мастер рад, под насловом **Права лица чији се подаци о личности обрађују од стране модела вештачке интелигенције** пријављен и одбрањен на Правном факултету Универзитета у Нишу:

- резултат сопственог истраживачког рада;
- да овај мастер рад у целини, нити у деловима, нисам пријављивала на другим факултетима, нити универзитетима;
- да нисам повредила ауторска права, нити злоупотребила интелектуалну својину других лица.

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

Аутор мастер рада: **Ленка Секулић**

У Нишу, _____

Потпис аутора
