

Софија МИЛЕНКОВИЋ¹

Министарство одбране

Проф. др Саша АТАНАСОВ²

Правни факултет Универзитета у Приштини

са привременим седиштем у Косовској Митровици

ДОИ: 10.5937/bezbednost2501123М

УДК: 004.8:35(497.11) 005.334:004.8

Прегледни научни рад

Примљен: 29. 4. 2024. године

Ревизија: 14. 3. 2025. године

Датум прихватања: 14. 3. 2025. године

Безбедносни аспекти употребе вештачке интелигенције у раду јавне управе

Апстракт: Посматрајући кроз призму државној, односно јавној сектора и уважавајући аргументе да се ради о комплексној, недовољно познатој и у великој мери јавно неретулисаној области, употреба вештачке интелигенције (ВИ) сагледава се у овом раду примарно кроз сферу пружања јавних услуга, размене и заштитне података, али и препознавања и превазилажења основних безбедносних ризика. Зависно од мотива и циљева са којима се користи, у раду се разматрају и позитивни и негативни аспекти употребе савремених информационо-комуникационих технологија, с акцентом на домаћима и ефектима ВИ. Долази се до закључка да је неопходно минимизирати безбедносне ризике, односно ојачати од злонамерној коришћења ВИ, јервенствено кроз обезбеђење свеобухватној институционалној и јавној оквира, адекватне подршке образованој и стручној кадра и институција и уз конјункцирања улаза у иновације, ради очувања поверења грађана у систем и институције.

Кључне речи: вештачка интелигенција (ВИ), јавна управа, јавни оквир, заштитна података, безбедносни ризици.

¹ sofijamilenkovic.fb@gmail.com, <https://orcid.org/0009-0002-3426-0487>.

² sasa.atanasov@pr.ac.rs, <https://orcid.org/0000-0003-0157-3049>.

Увод

Виртуелни свет представља чулну, дигиталну илузију стварног света (Мојси, 2016: 153). Процес дигитализације, као најважнији катализатор иновација и конкурентности, постао је основа дигиталне трансформације и употребе вештачке интелигенције (енг. *Artificial Intelligence* – AI) како на међународном, тако и на националном нивоу. С друге стране, појачано интересовање за нове технологије јесте не само покретач иновација, већ и међудржавних тензија, имајући у виду бројне пратеће ризике и друга питања која су од утицаја на националну безбедност.

Људска интелигенција, посматрана било с аспекта интелигенције појединаца, било с аспекта интелигенције друштва, подразумева искуствено учење из животних догађаја (Миливојевић, 2015: 229). Аналогно људској интелигенцији, концепт вештачке интелигенције (ВИ) начелно би подразумевао компјутерски програм који је способан да сам „креативно и искуствено размишља“ на бази сетова података и без додатних програмских инструкција. Од када је 1955. године математичар и информатичар Џон Макарти (*John McCarthy*) увео термин „вештачка интелигенција“, означавајући њиме јединство науке и инжењеринга у креирању интелигентних машина (Britannica, 2023), дефинисање појма ВИ стално је еволуирало. Данас, аутори који ВИ дефинишу с аспекта процеса размишљања и закључивања под њом подразумевају нове информационе системе и машине способне да самостално уче и предузимају различите активности онако како то чини интелигентно људско биће (Андоновић, 2020: 112), односно машине и информационе системе оспособљене да симулирају процесе људске интелигенције на основу одговарајућег алгоритма, кода или технике (Прља et al., 2020: 18).

Према дефиницији Европске комисије датој у Извештају о дефинисању вештачке интелигенције, под вештачком интелигенцијом подразумевају се системи који показују разумно, интелигентно понашање и који на основу анализе података из свог окружења

доносе одлуке са одређеним степеном аутономије, како би остварили одређене циљеве. Како на глобалном плану не постоји јединствено одређење појма ВИ, то је ова широко прихваћена дефиниција Европске комисије прихваћена и у *Стратегији развоја вештачке интелигенције у Републици Србији за период 2020–2025. године*.

Место вештачке интелигенције у раду јавне управе

Као научна дисциплина, ВИ је постала један од кључних покретача четврте индустријске револуције, захваљујући својој мултидисциплинарности. Свеукупно посматрано, за развој ВИ неопходно је коришћење људске интелигенције, машинског учења (као суштинске поддисциплине или подскупа ВИ), адекватне инфраструктуре и великог броја података (као основног ресурса машинског учења). Неопходно је и постојање одговарајућег правног оквира како би се обезбедила регулативна подлога за истраживање, развој и примену друштвено корисних решења заснованих на ВИ, уз уважавање чињенице да нове технологије надилазе традиционалне државне границе. Такође, како је развој нових технологија сложен и динамичан процес који је тешко нормативно-правно испратити, то је у домену ВИ, поред правне регулативе, све важнија улога универзалних пословних, етичких и моралних принципа и стандарда које доносе пословна и стручна удружења и организације (Прља et al., 2020: 18) и чије су процедуре доношења и измене знатно брже и једноставније.

Последње деценије XX века донеле су бројне промене на плану функционисања како целокупног друштва, тако и извршне власти; паралелно са технолошким развојем, глобализацијом и растућом улогом цивилног друштва, дошло је до брисања претходне јасне подељености владиног (енг. *government*), невладиног (енг. *nongovernmental organizations*) и приватног сектора, као и до појаве новог термина за процес управљања (енг. *governance*), за који не постоји адекватан или прецизан превод у српском језику (Давинић, 2008: 226). Суштински се под овим термином подразумева

новелирани концепт *јавне управе* као јавне службе и сервиса грађана, окренуте ка друштвеним потребама (Стојановић и Ђуровић, 2016: 13-14). Овакав концепт управљања подразумева сарадњу локалних, регионалних, државних и међудржавних ентитета у корист грађана и привреде, а у циљу уважавања универзалних вредности и промоције партнерства државног, цивилног и приватног сектора.

Имајући у виду комплексност предуслова потребних за развој и употребу ВИ у јавној управи и специфичности постојећих правних и друштвених система, и државе понаособ развијају сопствене програме, стратегије и технолошку инфраструктуру водећи рачуна о глобалним трендовима. Поједине европске државе, попут Естоније, у којој су дигитализација јавног сектора и технолошка оспособљеност службеника и грађана на изузетно високом нивоу (ова земља чак користи термин *Kratts* као синоним за ВИ, а што је име бића из њене митологије), имају за циљ да у што већој мери унапреде информационо-технолошку инфраструктуру ради ефикасне обраде великих количина података (OECD, 2019). Акцента чешког менаџмента је на рачунарским центрима високих перформанси за развој нових ВИ решења у јавном сектору (Европска комисија, 2022:29). Финска, као прва европска земља која је донела Стратегију за примену ВИ 2017. године и која слови за најнапреднију земљу у свету по колективним компетенцијама и практичној примени ВИ, већ више деценија континуирано улаже у образовну и иновациону политику, истраживања, развој науке и привреде, дигитално описмењавање грађана, креирање потребне инфраструктурне мреже и мреже тзв. паметних јавних услуга путем програма *Aurora AI*.

Уопштено посматрано, ВИ се најчешће користи у виду чет-ботова или виртуелних асистената који одржавају дијалог са корисницима јавних услуга; користи се и за анализу процеса преноса података и докумената кроз рачунарску мрежу, или у формату *Chat GPT* у циљу израде одређених дијаграма, слика и текстова, на основу одговарајућих упита. Такође, може вршити одабир кандидата за посао у складу са траженим карактеристикама. Основа је

и за рад апликација које имају потенцијал да користе методе „анонимизације и псеудонимизације“, тј. сакривања идентитета у складу са потребама корисника. Оно што је неспорно, а што је утврдио Глобални институт Макинси (*McKinsey Global Institute*) у својој оцени утицаја ВИ технологије на државну економију из 2018. године, јесте да ће имплементација ВИ највеће позитивне ефекте произвести у финансијском сектору, те да се до 2030. Године може очекивати да ће створити 13 трилиона америчких долара додатне вредности на глобалном нивоу, убрзавајући годишњи раст БДП-а за 1,2%.

На глобалном плану утврђен је *оксфордски индекс спремности за ВИ* као меродаван критеријум за упоређивање 39 индикатора на нивоу свих држава света, с акцентом на три стуба: 1. владин сектор (енг. *government*); 2. технолошки сектор; 3. подаци и инфраструктура (Oxford Insights, 2023: 22). Индекс представља поуздано мерило рада националних администрација и уједначен показатељ спремности приватног и јавног сектора и друштва у целини за технолошка решења заснована на ВИ. Основна идеја је да влада, тј. извршна власт, мора имати стратешку визију о развијању и управљању ВИ, утемељену на одговарајућим јавним политикама, правним и етичким принципима, адекватним дигиталним капацитетима, новим технологијама и стручним кадровима. Није занемарена ни важност висококвалитетних података као веома важног ресурса за ВИ и за унапређење јавних услуга. Према Оксфордском извештају о оцени спремности држава за ВИ у 2019. години Република Србија је била на 58. месту (од 194 држава), 2020. године на 46. месту (од 172 рангиране државе), а 2023. и 2024. године на 57. месту (од 193, односно 188 држава); на првом месту су САД, првенствено захваљујући развијености технолошког сектора. Важно је истаћи да је према Оксфордском извештају о оцени спремности држава за ВИ из 2023. године Србија апострофирана као тек друга држава у региону Источне Европе која је, после Руске федерације (РФ), усвојила етичке смернице за примену ВИ.

ВИ је додатно добила на значају у 2023. години, када је постала саставни део међународне развојне агенде. *Закон о вештачкој*

интелигенцији (ВИ) донет на нивоу Европске уније (*The EU's AI Act*) у марту 2024. године, чија се пуна примена, уз одређене изузетке, очекује од 2. августа 2026. године, за сада представља први и једини правни оквир који се бави ризицима ВИ, уједно дајући земљама Европске уније водећу улогу у овој области (Oxford Insights, 2023: 21-22). Законом се штите основне демократске вредности, владавина права и еколошка одрживост у областима које су везане за ВИ, уз истовремено подстицање иновација и промовисања европских земаља као лидера у овој области. Намера је да овај закон постане глобални стандард на основу којег се утврђује у којој мери ВИ има позитиван, а у којој негативан утицај на људске животе, као и на државне системе.

Вештачка интелигенција и заштита података у правном систему Републике Србије

Како у правном систему Републике Србије не постоји законска дефиниција појма јавне управе, већ само дефиниција државне управе (под којом се, сагласно са Законом о државној управи, подразумевају министарства, органи управе у саставу министарства и посебне организације), различити аутори је различито дефинишу. Примера ради, с аспекта карактера њене делатности, јавна управа се може дефинисати као скуп органа и организација који врше власт, групу функција и задатака усмерених на вршење оних делатности које из било ког разлога грађани не могу обављати сами за себе (Кавран, 2003: 51). С аспекта делокруга, јавна управа, поред државних органа, обухвата и органе покрајинске аутономије и локалне самоуправе, као и јавна предузећа, службе и установе ван привреде.

У правном систему Републике Србије преображај државне управе ка моделу јавне управе започет је доношењем најпре *Стратегије реформе државне управе 2004. године* и акционих планова за њено спровођење (2004-2008. године, 2009-2012. Године), а потом *Стратегије реформе јавне управе Републике Србије 2014. године* и акционог плана за њено спровођење (2015-2017. године). Убрзо

након доношења ових стратешких докумената усвојен је и нови *Закон о ојшћем уйравној йосйууку (ЗУП)* 2016. Године, с циљем успостављања модерне, добре јавне управе, утемељене на теоријском концепту који сагледава управу као сервис грађана и привреде. Новим Законом уведен је и потпуно нов правни институт – *јединсйвено уйравно месйо*, са идејом да грађани добију модерну, дигитализовану и делотворну управу, која ће пружати услуге грађанима и привреди у тачно спецификованом физичком или дигиталном простору. Као најважнији предуслови који морају бити испуњени да би овај институт заживео у пуном обиму препознати су: 1) одговарајућа инфраструктура; 2) едукација државних службеника и грађана и 3) постепени прелазак на услуге електронске управе. Већ 2018. године донет је *Закон о електйронској уйрави* с циљем да уреди електронско управно поступање органа јавне управе, односно обављање послова из њиховог делокруга и размена података употребом информационо-комуникационих технологија. На овај начин створена је полазна основа за делотворан даљи рад електонске управе (е-управе) и даљи развој ВИ у тој области. Доношењем *Стйрайћеије реформе јавне уйраве у Рейублици Србији за йериод од 2021. до 2030. йодине*, као посебни циљеви рада јавне управе дефинисани су ефикасно и економично пружање услуга грађанима кроз унапређење и оптимизацију већ постојећих услуга, на основу коришћења великих сетова података, ВИ и блокчејн технологије.

Однос јавне управе и ВИ добио је значајно место у *Стйрайћеији развоја вешййачке инйтелиенције у Рейублици Србији за йериод 2020-2025. йодине*. Према Стратегији, интелигентна решења, поред пружања подршке корисницима, обезбеђују персонализацију услуга, поједностављују управне процедуре и убрзавају многе рутинске поступке, посебно у случајевима када су подаци већ похрањени у електронским регистрима и евиденцијама органа. Како се истиче на Националној платформи за вештачку интелигенцију, за то су основни предуслови: обезбеђење поузданости примењених решења, заштита приватности података, као и вишеканални приступ и обезбеђење потребне интеракције ВИ, грађана и службеника.

Изазов који је идентификован у регулаторном стратешком оквиру тиче се достизања равнотеже између прописа у области заштите података о личности и креирање простора за развој ВИ и иновација. С тим у вези, заштиту приватних података и спречавања злоупотреба нових технологија гарантује *Закон о заштити података о личности*, који у члану 4 дефинише о којим је тачно подацима реч. За потребе нашег правног система одређење *појма податка*, као нужног ресурса за коришћење ВИ, даје важећи *Закон о електронској управи* у 4. члану.

Усвајањем Београдске министарске декларације у области вештачке интелигенције у децембру 2024. године, на предлог Републике Србије и уз сагласност 44 државе чланице Глобалног партнерства за вештачку интелигенцију и Европске уније, указано је на значај механизма којима ће ВИ бити правно и етички регулисана и на важност јавног дељења информација и резултата рада у овом домену у циљу смањења технолошких разлика међу државама; издвојени су и кључни приоритети за будућност ВИ, укључујући очување индивидуалних слобода, људских права, заштита приватности, промовисање сигурне и одрживе ВИ, и друго (Национална платформа за вештачку интелигенцију, 2024).

Безбедносни ризици употребе вештачке интелигенције у раду јавне управе

Поред тога што су креатори ВИ претежно компаније које комерцијално или некомерцијално дистрибуирају производе и услуге засноване на ВИ (Гугл, Мета, Тесла и др.), ту улогу могу преузети и државе, које појединачно или у сарадњи са другим државама или компанијама креирају, примењују и контролишу системе ВИ (Прља et al., 2020: 8). У области јавног сектора и државне администрације уочен је глобални пораст употребе нових технологија у 2023. години за око 10% (посматрано у односу на укупно 136,4 милиона запослених), и то нарочито у аналитичке сврхе, у циљу коришћења нових сервиса и апликација попут услуга е-трговине, ради унапређења сајбер безбедности и заштите путем енкрипције,

као и ради додатне едукације запослених (World Economic Forum, 2023). У Извештају Центра за четврту индустријску револуцију о десет најбољих нових технологија које значајно утичу на економију и друштво из 2024. године, на прво место стављена је ВИ која се користи за научна открића, захваљујући оствареном напретку у дубоком учењу и генеративној вештачкој интелигенцији (Centre for the Fourth Industrial Revolution, 2024). ВИ се користи и у законодавном процесу: у децембру 2023. године у Бразилу је усвојен закон који је у потпуности написала ВИ (Политика, 2023). Такође, ВИ се може у све већем обиму користити у циљу идентификовања недостатака како правног, тако и финансијског, здравственог и другог система. С друге стране, како наводи Џонатан Рајхентал (*Jonathan Reichental*, 2022), један од лидера у овој области, најкритичнији сегмент употребе ВИ у јавном сектору представља управљање подацима и информацијама, имајући у виду да овом аспекту 91% руководилица придаје кључни значај. Недостатак разноликости у подацима унетим у алгоритмат ВИ може, између осталог, утицати на појаву пристрасности у закључивању, или на појаву дискриминације по различитим основама (Ковачевић и Демић, 2023: 687).

Сложеност концепта ВИ указује на неопходност интердисциплинарног инклузивног приступа у њеном разумевању, у контексту појединачног и општег добра. Као најчешће препреке за примену ВИ наводе се: инфраструктурни недостаци, мањак напредне технолошке опреме, недостатак едукованих кадрова, етички и правни изазови и отежана контрола протока информација (Зоин, 2023: 14). Када говоримо о државним и друштвеним системима, рањивости су највидљивије у области заштите података о личности, у систему националне безбедности (на пример, због развоја оружаних система са ВИ), социјалне заштите и запошљавања (услед појављивања нових занимања и потребе за преквалификацијом), у образовном систему (због прекомерног коришћења *Chat GPT*-ја, довођења у питање академског и научног интегритета, и слично), у области етичких и моралних стандарда и норми (услед губљења границе између јавне и приватне, односно личне сфере), системима преноса података

(као што су извлачење и класификовање података доступних на друштвеним мрежама, генерисање података и информација које могу бити нетачне, непотпуне, непримерене, осетљиве, поверљиве или политички контроверзне), на безбедносном и одбрамбеном плану (примера ради, услед сајбер напада), и друго.

Неадекватна и недовољна контрола протока података и информација у сајбер простору убрзано је постала водећи безбедносни ризик у коришћењу ВИ. Због чињенице да је контрола протока информација постала глобални изазов, појачана је сарадња међународних актера (Путник, 2022: 14), али је отворен и нови фронт за међудржавне сукобе. Сагласно наведеном, квалитетна организација информационог система, ради обезбеђења добре основе за борбу против људских и системских грешака на државном, као и међудржавном нивоу, обезбедила би свођење потенцијалних ризика на минимум (Протић, 2013). Европска комисија сматра да ће 5G инфраструктура, као технологија следеће генерације, омогућити повезивање великог броја апликација, индивидуалних корисника и појединих сектора (образовања, безбедности, здравства, итд.), али да ће, с друге стране, отворити пут за злоупотребу података, односно системско и изузетно брзо ширење дезинформација коришћењем ВИ (NALED et al., 2022). Примера ради, због серије сајбер напада на сервер албанске владе *administrata.al*, на владин портал *e-Albania.al* и на систем за управљање информацијама *TIMS* албанска влада је 6. септембра 2022. године прекинула дипломатске односе са Исламском Републиком Иран, наводећи да је тиме угрожена национална безбедност, иако напади нису довели до „значајног цурења података“ (Elezi, Gholami, 2022). У накнадним истрагама САД и Републике Албаније откривено је да су хакерске групе из Ирана стајале иза овог напада, за који је наводни повод било присуство око 3.000 припадника народних муџахедина Ирана (МЕК) на територији Албаније, а које Техеран сматра терористичком организацијом, што је иранско Министарство спољних послова негирало.

У последње две деценије нова технологија добија све значајнију улогу у спровођењу изборних кампања, манипулисању ин-

формацијама и грађанима и селектовању бирача по различитим критеријумима, на основу лако доступних личних података. Године 2016. први пут је на глобалном плану актуелизовано питање неоправданог коришћења модерних технологија у спровођењу кампање око референдума о Брегзиту, као и председничких избора у САД 2016. године, због постојања доказа да су технологије засноване на ВИ злоупотребљаване за манипулације грађанима, као и да су око петине свих политичких твитова поставили ботови (Полонски, 2017). Наиме, током председничких избора 2016. године у САД покренута је опсежна маркетиншка кампања која је циљала на одређену групу потенцијалних гласача Доналда Трампа, узимајући у обзир њихове индивидуалне преференције и психолошке профиле, како би се пронашао адекватан емоционални покретач за сваког од њих. Радило се о софистицираној операцији микроциљања, уз ослањање на велике податке, недовољно уређен правни систем и машинско учење, с циљем да се понашање људи окрене у жељеном смеру. Бирачи су добијали поруке на основу предвиђања њихове подложности одређеним аргументима. Паралелно са тим, амерички председнички избори 2016. године изнели су на међународну сцену феномен „лажних вести“, најпре пласирањем дезинформације да је папа Фрања подржао кандидатуру Доналда Трампа у финалу изборне кампање (Полонски, 2017), да би се потом политизацијом овог термина од стране самог Трампа тежило дискредитацији естаблираних медија. „Лажне вести“ су 2017. Године проглашене за „речи године“, а те године је употреба поменутог термина порасла за 365% у односу на 2016. годину (*Collins Dictionary*). Овакав след догађаја био је резултат политичких дешавања која су обележила 2016. годину и отворио је питање етичности и законитости коришћења ВИ, али и питање заштите сета основних људских права (попут права на приватност). Иако су паралелно заживели софтвери за откривање дезинформација које су развиле новинске куће попут Дојче Велеа (*Deutsche Welle, DW*) или руске новинске агенције ТАСС, показало се да ни они не дају 100% тачне резултате. С тим у вези је у сврху спречавања ширења

дезинформација и злоупотреба генеративне ВИ у политичке сврхе био активиран Оперативни центар за изборе за Европски парламент одржане јула 2024. године, како би се идентификовале потенцијалне претње у реалном времену (Гајић, 2024). Такође, Мета, Мајкософт, Опен АИ и 17 других технолошких компанија сагласиле су се да ће заједнички радити на спречавању негативног утицаја ВИ на изборе широм света у 2024. години (Гајић, 2024).

Свеукупно посматрано, проблем није у самој технологији, већ у начину и сврси њеног коришћења. Иако је настанак ВИ утемељен на објективним основама, чињеница је да су је створили људи који су инхерентно пристрасни. Примера ради, ВИ дизајнирана за откривање рањивости друштвених или државних система неке земље, може бити искоришћена за уклањање спорног садржаја или новооткривене мане безбедносног система, али исто тако може бити експлоатисана од стране оних који је примарно контролишу, тако што ће се лажна вест или откривена нерегуларност злонамерно искористити као предност. Поступак компаније Гугл из јуна 2023. године, која је издала саопштење да ће податке корисника њених јавно доступних сервиса убудуће користити за тренирање својих модела ВИ, апострофирао је опасности од злоупотреба ВИ на свим нивоима. Како стручњак за сајбер безбедност Брус Шнајер (*Bruce Schneier*) истиче, проблем је и у томе што сама ВИ може доћи до жељеног резултата или циља на начин на који њени дизајнери нису желели, примарно захваљујући латентној двосмислености сложених друштвених система, конкретном контексту и карактеру информација (2023: 229-240).

Због реалне опасности од могућих злоупотреба, неопходни су додатни напори на унапређењу институционалних оквира и целокупне правне регулативе у области информационо-комуникационих технологија (ИКТ), сајбер простора, ВИ и сл., уз отклањање постојећих административних и техничких оптерећења и ограничења. Као нарочито осетљива намеће се потреба заштите података о личности у ситуацијама њихове аутоматске обраде, објављивања, систематског прикупљања, преношења и складиштења од

стране појединаца и органа власти, сагласно са чланом 8 Европске конвенције о људским правима којима је регулисана заштита личних података (ReSPA, 2017: 63-69). Суштина је у онемогућавању злонамерног коришћења ВИ, спречавању повреде основних људских права и ширења неистинитих информација и полуинформација помоћу нових технологија које могу произвести изузетно лоше последице по појединца и друштво – попут подстицања насиља, утицаја на изборе, губитка поверења у државни и друштвени систем (Ковачевић и Демић, 2023: 702). Ипак, иако је Акциони самит за вештачку интелигенцију (*Artificial Intelligence Action Summit*) одржан у Паризу почетком фебруара 2025. године резултирао сагласношћу по питању важности безбедносног аспекта ВИ, указао је на озбиљну подељеност водећих држава по питању детаљног уређења и нормирања ове области, с обзиром на противљење САД и Велике Британије да усвоје Декларацију са овог самита, између осталог, због забринутости да би прекомерна регулација могла угушити иновације и развој технологије. С друге стране, Декларацију је потписало 60 земаља, међу којима су Кина, Индија, Канада и Француска.

Оно што је неспорно, јесте значај ВИ за друштво у целини, због чега акценат треба ставити на њено системско коришћење у јавном и приватном интересу и на темељу сарадње јавног и приватног сектора, образовних и научних установа и појединаца. Уједно, не треба занемарити извесност и учесталост нежељених ефеката, неетичког коришћења, као ни далекосежност и озбиљност последица злоупотреба ВИ како на рачун појединаца, тако и на рачун политичко-безбедносних, друштвених, финансијских, административних и других система (NALED et al., 2022: 22-24).

Закључак

Вештачка интелигенција, захваљујући размерама и домаћинству утицаја на државу и друштво, може значајно допринети ефикасности рада јавне управе и квалитету услуга које држава пружа грађанима и привреди. Њена ефикасна, делотворна и безбедна

примена подразумева испуњење сета (пред)услова, попут одговарајућих ИКТ система, јаких и стабилних институција, дигитално писмене и информисане државне и привредне структуре и појединце, који поред потребних знања имају и изграђено поверење у нове технологије. Упркос бројним позитивним ефектима употребе ВИ у јавној управи, њени потенцијали нису у довољној мери искоришћени, у првом реду из безбедносних, правних, инфраструктурних и институционалних разлога. С правног и безбедносног аспекта, питања злонамерног коришћења ВИ, односно дезинформисања и угрожавања безбедности уз помоћ ВИ могла би, теоретски, бити решена одговарајућом законском регулативом која би омогућила санкционисање злоупотреба дигиталног простора и ВИ, као и ефикаснијим правним регулисањем прикупљања, коришћења и размене података, како би се заштитила сфера приватности. Ипак, с обзиром на брзину развоја ВИ, с једне стране, и трајање и комплексност процеса доношења прописа, с друге стране, несумњиво је да ће законодавство увек бити у заостатку за друштвеним развојем и технологијом, због чега је у пракси све чешће ослањање на универзалне пословне, етичке и моралне принципе и стандарде релевантних тела, односно организација.

У циљу успостављања неопходног институционалног и инфраструктурног оквира једно од решења било би развијање већег броја тела и структура јавне управе на ресорном нивоу, специјализованих за сајбер безбедност и ВИ и са фокусом на милтидисциплинарном, координисаном и транспарентном приступу. Такође, један од предлога била би измена законског оквира о заштити података о личности како би се заштитиле и санкционисале евентуалне злоупотребе у овом домену и извршила детаљна класификација података према веродостојности, релевантним корисницима и степену поверљивости. Уз то, сарадња јавног, приватног и цивилног сектора јесте неминовност како би се путем размене искустава сагледале све предности и ризици нових технологија.

Литература

1. Андоновић, С. (2020). Стратешко-правни оквир вештачке интелигенције у упоредном праву. Страни правни живот, 64(3): 111-123.
2. Artificial Intelligence Action Summit, <https://www.elysee.fr/en/sommet-pour-l-action-sur-l-ia>. доступан: 12. 2. 2025.
3. Благојевић, М. С. (1995). Право и стварност. „Службени лист СРЈ“, Београд.
4. Britannica, John McCarthy, American mathematician and computer scientist: доступан: <https://www.britannica.com/biography/John-McCarthy>.
5. Centre for the Fourth Industrial Revolution. World Economic Forum. Top 10 Emerging Technologies of 2024. Flagship Report, June 2024, https://www.weforum.org/publications/top-10-emerging-technologies-2024/in-full/introduction-emerging-technologies-2024/?gad_source=1&gclid=EAIaIQobChMIo4KwhOOEjAMVBqQDBx2OwiuMEAAAYASAAEgK0DPD_BwE. доступан 1. 3. 2025.
6. Davinić, М. (2008). Importance of nation-state in the globalized world. Annals of the Faculty of Law in Belgrade, Belgrade Law Review, Journal of Legal and Social Sciences University of Belgrade, Vol. 3. p.p. 216-235.
7. Гајић, Н. (2024). Мета формира тим за борбу против дезинформација и злоупотребу AI. PC Press. <https://pcpress.rs/meta-formira-tim-za-borbu-protiv-dezininformacija-i-zloupotrebu-AI/>. доступан 12. 12. 2024.
8. Elezi, E., Gholami, N. (2022). Albania blames Iran for cyberattacks. Deutsche Welle (DW), <https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285>. доступан 16. 6. 2024.
9. European Commission, Directorate-General for Communication (2018). A definition of AI: Main capabilities and scientific disciplines. Brussels, https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_AI_18_december_1.pdf. доступан 29. 7. 2024.

10. European Commission. (2022). AI Watch European Landscape on the Use of Artificial Intelligence by the Public Sector. JRC Science for Policy Report, <https://op.europa.eu/en/publication-detail/-/publication/7ed5aa59-dca1-11ec-a534-01aa75ed71a1/language-en>. доступан 17. 5. 2024.
11. European Commission, JRC Science for Policy Report (2022). AI Watch, European Landscape on the use of Artificial Intelligence by the Public Sector. Luxemburg. <https://op.europa.eu/en/publication-detail/-/publication/7ed5aa59-dca1-11ec-a534-01aa75ed71a1/language-en>. доступан 3. 2. 2024.
12. European Parliament, EU Artificial Intelligence Act: first regulation on artificial intelligence, <https://artificialintelligenceact.eu/>. доступан 30. 9. 2024.
13. Закон о државној управи, Службени гласник Републике Србије, бр. 79/2005, 101/2007, 95/2010, 99/2014, 47/2018 и 30/2018 – др. закон.
14. Закон о електронској управи, Службени гласник Републике Србије, број 27/18.
15. Закон о информационој безбедности, Службени гласник Републике Србије, бр. 6/2016, 94/2017 и 77/2019.
16. Закон о заштити података о личности, Службени гласник Републике Србије, број 87/18.
17. Закон о општем управном поступку, Службени гласник Републике Србије, бр. 18/2016-10, 95/2018-441 (Аутентично тумачење), 2/2023-44 (УС).
18. Зоин, М. (2023). ChatGPT од почетника до професионалца. Компјутер библиотека, Београд.
19. Интернет презентација Националне платформе за вештачку интелигенцију, <https://www.ai.gov.rs>. доступан 30. 12. 2024.
20. Интернет презентација владе Републике Србије, www.gov.rs. доступан 16. 6. 2024.
21. Интернет презентација Републичког завода за статистику. <https://www.stat.gov.rs/sr-latn/oblasti/upotreba-ikt/upotreba-ikt-rojedinci/>. доступан 15. 6. 2024.

22. Jonathan Reichental. (2022). 10 reasons why data governance must be your priority in 2023. <https://www.reichental.com/2022/12/27/10-reasons-data-governance-must-be-your-priority/>. доступан 26. 4. 2024.
23. Кавран, Д. (2003). Јавна управа, Реформа, тренинг, ефикасност. Савет за државну управу Владе Републике Србије, Удружење за јавну управу Србије, Факултет организационих наука Универзитета у Београду и Центар за јавну управу, у сарадњи са Фондом за подизање капацитета Програма за развој Уједињених нација у Србији и Црној Гори, Београд.
24. Ковачевић, А., Демић, Е. (2023). Вештачка интелигенција за откривање лажних вести на социјалним медијима – испитивање ставова. Међународни проблеми, 75 (4): 685-710.
25. Stojanović, B., Đurović, G. (2016). Comparative Study with Baseline Analysis. Regional School of Public Administration in the Western Balkan Region, ReSPA, Podgorica.
26. Миливојевић, З. (2015). Уловити љубав. Психополис, Нови Сад.
27. Mc Kinsey & Company, MCKiney Global Institute. <https://www.mckinsey.com>. доступан 18. 9. 2024.
28. Мојси, Д. (2016). Геополитика телевизијских серија или победа страха. Clio, Београд.
29. NALED, Влада РС, Startech, Philip Morris AD Niš. (2022). Анализа стања иновација и процеса дигиталне трансформације у Републици Србији, <https://startech.org.rs/htdocs/Files/01155/Analiza-stanje-inovacija-i-procesa-digitalne-transformacije-u-Republici-Srbiji.pdf>. доступан 15. 3. 2024.
30. OECD. Report of Estonia's AI Taskforce, <https://www.oecd-events.org/smart-data-and-digital-technology-in-education/session/9c091662-e417-ed11-bd6e-a04a5e7d2ab9/report-of-estonia-s-ai-taskforce>. доступан 20. 2. 2024.
31. Oxford Research Encyclopedias. <https://dictionary.cambridge.org/dictionary/>. доступан 27. 5. 2024.
32. Oxford Insights. Government AI Readiness Index 2023, <https://oxfordinsights.com/ai-readiness/ai-readiness-index/>. доступан 19. 4. 2024.

33. Oxford Insights. Government AI Readiness Index 2024, <https://oxfordinsights.com/ai-readiness/ai-readiness-index/>. доступан 10. 3. 2025.
34. Политика (2023). У Бразилу усвојен закон који је у потпуности написала вештачка интелигенција, <https://www.politika.rs/scc/clanak/588046/U-Brazilu-usvojen-zakon-koji-je-u-potpunosti-napisala-vestacka-inteligencija>. доступан 20. 2. 2024.
35. Polonski, V. (2017). The good, the bad and the ugly uses of machine learning in elections campaign. Centre for Public Impact, <https://www.centreforpublicimpact.org/insights/good-bad-ugly-uses-machine-learning-election-campaigns>. доступан 27. 2. 2024.
36. Протић, Д. (2013). Информациона безбедност: стандарди или правила. Војно дело, 65 (1), 133-150.
37. Прља, Д., Гасми Г., Кораћ, В. (2020). Људска права и вештачка интелигенција. Институт за упоредно право, Београд.
38. Путник, Н. (2022). Сајбер рат и сајбер мир. Универзитет у Београду - Иновациони центар Факултета безбедности. Академска мисао, Београд.
39. Schneier, B. (2023). A Hacker's Mind, W. W. Norton & Company, Inc., New York.
40. Стратегија развоја вештачке интелигенције у Републици Србији за период 2020-2025. године, Службени гласник Републике Србије, број 96/19-5.
41. Стратегија реформе јавне управе у Републици Србији за период од 2021. до 2030. године, Службени гласник Републике Србије, бр. 42/2021-1 и 9/2022-54.
42. World Economic Forum. The Future of Jobs Report, <https://www.weforum.org/publications/the-future-of-jobs-report-2023/>. доступан 24.10.2024.

Security Aspects Related to State Administration Use of Artificial Intelligence

Abstract: *Through the scope of the state, viz. the public sector and taking into account the fact that it is a complex, not sufficiently familiar and, to a large extent, legally underregulated area, this paper explores the use of artificial intelligence (AI) not only through the sphere of public service provision, and exchange and protection of data, but also recognizing and overcoming core security risks. In line with the respective motives and goals of application, the paper discusses both positive and negative aspects of modern information and communication technologies, focusing on the scope and effects of AI. Despite the numerous positive effects of using AI in public administration, its potential has not been sufficiently exploited, primarily because of security, legal, infrastructural and institutional reasons. The essence is to prevent the malicious use of AI, prevent the violation of fundamental human rights and the spread of disinformation and misinformation using new technologies that can have extremely bad consequences for the individual and society.*

Considering the complexity of the legislative process, there is an increasing reliance on universal business, ethical and moral principles and standards of relevant bodies, i.e. organizations in practice. The ultimate conclusion made is that it is necessary to minimize security risks and the dangers of malicious use of AI, primarily by establishing comprehensive institutional and legal frameworks, providing adequate support from expert personnel, private and public institutions and continuous investment in innovation, in order to ensure the popular trust in the system and its institutions.

Although there is no global agreement about the basic principles of using AI in practice, the Republic of Serbia follows the standards and policies of the EU member states, which advocate legal regulation of this area, adequate data protection, and the cooperation of public administrations at the international level.

Keywords: *artificial intelligence (AI), public administration, legal framework, data protection, security risks*