

Карповачки лист



СРЕМСКИ КАРЛОВЦИ, 2026.



МЕДИЈИ И ЗАШТИТА ПРИВАТНОСТИ У ДИГИТАЛНОМ ДОБУ:

импликације за људска права
и сигурност података

Специјално издање

КАРЛОВАЧКИ ЛИСТ 021

МЕДИЈИ И ЗАШТИТА
ПРИВАТНОСТИ У
ДИГИТАЛНОМ ДОБУ:
ИМПЛИКАЦИЈЕ ЗА ЉУДСКА
ПРАВА И СИГУРНОСТ
ПОДАТАКА

Сремски Карловци, 2026.

Карловачки лист 021

Медији и заштита приватности у дигиталном добу:
импликације за људска права и сигурност података

Сремски Карловци
Србија

Издавач:
Центар за културу, едукацију и медије „Академац”
Сремски Карловци

За Издавача:
Др Александра Пењишевић

Главни и одговорни уредник:
Др Бранислав Санчанин

Графички дизајн:
Јелена Николић

Карловачки лист је уписан у
Регистар медија: NV 000939

ISSN 2956-0217 = Карловачки лист 021

Штампа:
PROOF, Београд, Пива Караматијевића 12/9

Тираж: 700

Штампање специјалног издања Карловачког листа 021
подржало је Министарство информисања и
телекомуникације Републике Србије

Издавачки савет:

Проф. др Александра Пењишевић, Београд, Србија

Проф. др Бранислав Санчанин, Београд, Србија

Проф. др Марина Бугарчић, Београд, Србија

Проф. др Владимир Кнежевић, Београд, Србија

Проф. др Маргарита Богданова, Свищов, Бългaрия

Проф. др Роберт Димитровиски Скопје, Северна Македонија

Доц. др Милица Денковска, Штип, Северна Македонија

Доц. др Анита Димитријовска-Јанкуловска, Скопје, Северна Македонија

Проф. др Катарина Стојановић, Нови Сад, Србија

Проф. др Бориша Лечић, Нови Сад, Србија

Проф. др Бранислав Ранђеловић, Лепосавић, Србија

Проф. др. Евелина Парашкевова - Великова, Свищов, Бългaрия

Доц. др Душан Симјановић, Ниш, Србија

Проф. др Иван Блажевски, Скопје, Северна Македонија

Проф. др Немања Деретић, Београд, Србија

Садржај

УВОДНА РЕЧ УРЕДНИКА	9
УТИЦАЈ МЕДИЈСКЕ ПИСМЕНОСТИ НА ПЕРЦЕПЦИЈУ РИЗИКА И ЗАШТИТУ ПРИВАТНОСТИ ГРАЂАНА	11
УВОД	12
ПРЕГЛЕД ЛИТЕРАТУРЕ	13
ЗАШТИТА ПРИВАТНОСТИ КОРИСНИКА НА ДРУШТВЕНИМ МРЕЖАМА	14
ЗАКЉУЧАК	17
РЕФЕРЕНЦЕ	17
УТИЦАЈ ДРУШТВЕНИХ МЕДИЈА НА МЕНТАЛНО ЗДРАВЉЕ МЛАДИХ: МУЛТИДИМЕНЗИОНАЛНИ ПРИСТУП	19
УВОД	20
ДРУШТВЕНЕ МРЕЖЕ: ПОЗИТИВНЕ ИМПЛИКАЦИЈЕ НАСУПРОТ НЕГАТИВНИХ ИМПЛИКАЦИЈА	21
ЗАКЉУЧАК	25
РЕФЕРЕНЦЕ	25
АЛГОРИТАМСКА ПЕРСОНАЛИЗАЦИЈА И ЗАШТИТА ПРИВАТНОСТИ У ДИГИТАЛНИМ МЕДИЈИМА	27
УВОД	28
ДИГИТАЛНИ МЕДИЈИ КАО ИНФРАСТРУКТУРА ПРИКУПЉАЊА ПОДАТАКА	29
Алгоритамско профилисање, персонализација и јавно мњење	29
ПРИВАТНОСТ, БЕЗБЕДНОСТ ПОДАТАКА И ПРАВО НА КОНТРОЛУ	30
Вештачка интелигенција, deepfake садржаји и нови ризици	31
Регулаторни оквир и одговорност дигиталних платформи	32
Етички изазови медија и дигиталног оглашавања	33
МОДЕЛ ОДГОВОРНЕ ДИГИТАЛНЕ КОМУНИКАЦИЈЕ	34
ЗАКЉУЧАК	37
РЕФЕРЕНЦЕ	37
УПОТРЕБА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У НОВИНСКИМ РЕДАКЦИЈАМА И РИЗИЦИ ПО ПРИВАТНОСТ ГРАЂАНА	39
УВОД	40
МЕТОДОЛОГИЈА РАДА	41
ПРИМЕНА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У НОВИНСКИМ РЕДАКЦИЈАМА	42
РИЗИЦИ ПО ПРИВАТНОСТ ГРАЂАНА И ИЗВОРА	44
ПРАВНИ И ЕТИЧКИ ОКВИР УПОТРЕБЕ ВИ У НОВИНАРСТВУ	47
ЗАКЉУЧАК	51
РЕФЕРЕНЦЕ	52
МЕДИЈСКА РЕПРЕЗЕНТАЦИЈА И ДИГИТАЛИЗАЦИЈА АРХИТЕКТОНСКОГ НАСЛЕЂА НАЦИОНАЛНИХ МАЊИНА ВОЈВОДИНЕ И САВРЕМЕНЕ ИНТЕРПОЛАЦИЈЕ	53
УВОД	54
ИСТОРИЈСКИ КОНТЕКСТ И ПРЕДУСЛОВИ СТВАРАЊА АРХИТЕКТУРЕ	
НАЦИОНАЛНИХ МАЊИНА	54
КРИТЕРИЈУМИ И ТИПОЛОШКА АНАЛИЗА	55
РЕЗУЛТАТИ И ДИСКУСИЈА	56
УПОРИШТЕ У НАРОДНОЈ АРХИТЕКТУРИ КРОЗ НОВЕ МЕДИЈЕ	56
САВРЕМЕНЕ МЕДИЈСКЕ ТЕХНОЛОГИЈЕ И ИНТЕРПОЛАЦИЈА У РЕГИОНАЛНОМ СТИЛУ	57
ЗАКЉУЧЦИ	58
ЗАХВАЛНИЦА	58
РЕФЕРЕНЦЕ	59
ДИГИТАЛНИ МЕДИЈИ И МУЗИЧКА ИНДУСТРИЈА: ЗАШТИТА ПРИВАТНОСТИ КОРИСНИКА НА СТРИМИНГ ПЛАТФОРМАМА	60
УВОД	61
ДИГИТАЛНА ТРАНСФОРМАЦИЈА МУЗИЧКЕ ИНДУСТРИЈЕ	62

СТРИМИНГ ПЛАТФОРМЕ, АЛГОРИТМИ И ПЕРСОНАЛИЗАЦИЈА	63
ПОДАЦИ КОРИСНИКА И ПИТАЊЕ ПРИВАТНОСТИ	65
ПРАВНИ ОКВИРИ ЗАШТИТЕ ПОДАТАКА МОГУЋА РЕШЕЊА И ПРЕПОРУКЕ	66
ЗАКЉУЧАК	68
РЕФЕРЕНЦЕ	69
АЛГОРИТМИ У МЕДИЈИМА И ПРИВАТНОСТ ГРАЂАНА:	
АНАЛИЗА САВРЕМЕНИХ КИНЕСКИХ ИСТРАЖИВАЊА	71
УВОД	72
ТЕОРИЈСКИ ОКВИР	72
ВИ МЕДИЈИ И ПОВЕРЕЊЕ ЈАВНОСТИ	74
НЕУРОКОГНИТИВНИ АСПЕКТИ ПОВЕРЕЊА: ШТА МОЗАК ГОВОРИ О ВИ САДРЖАЈИМА?	76
УСВАЈАЊЕ ВИ НОВИНАРСТВА ИЗ ПЕРСПЕКТИВЕ НОВИНАРА	78
О ВЕШТАЧКОЈ ИНТЕЛИГЕНЦИЈИ У КИНЕСКИМ МЕДИЈСКИМ КУЋАМА:	
ПРИЈАТЕЉ ИЛИ НЕПРИЈАТЕЉ?	79
ИСТРАЖИВАЊЕ О ПРИМЕНИ ВИРТУЕЛНИХ ВОДИТЕЉА ЗАСНОВАНИХ НА	
ГЕНЕРАТИВНОЈ ВЕШТАЧКОЈ ИНТЕЛЕГЕНЦИЈИ У ИЗВЕШТАВАЊУ	81
ОД МЕДИЈСКЕ КА АЛГОРИТАМСКОЈ ПИСМЕНОСТИ – УМЕСТО ЗАКЉУЧКА	82
РЕФЕРЕНЦЕ	84
ПРЕТПОСТАВКА НЕВИНОСТИ У ДИГИТАЛНИМ МЕДИЈИМА У СРБИЈИ:	
АНАЛИЗА НАСЛОВА И ЛИДА НА ПОРТАЛИМА	85
УВОД	86
ТЕОРИЈСКИ ОКВИР	86
МЕТОДОЛОГИЈА ИСТРАЖИВАЊА	88
КВАЛИТАТИВНА АНАЛИЗА И ДИСКУСИЈА	92
ЗАКЉУЧАК	94
РЕФЕРЕНЦЕ	95
ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА, АЛГОРИТМИ И ПРИВАТНОСТ ГРАЂАНА	98
УВОД	97
ОД ДИГИТАЛНОГ ТРАГА ДО АЛГОРИТАМСКОГ ПРОФИЛА	99
КАДА АЛГОРИТАМ „ЗНА” ОНО ШТО МУ НИСМО РЕКЛИ	101
АЛГОРИТМИ КАО ПОСРЕДНИЦИ ИНФОРМАЦИЈА	102
ОД ПРОФИЛА КОРИСНИКА ДО ПЕРСОНАЛИЗОВАНОГ ИНФОРМАЦИОНОГ ОКРУЖЕЊА	103
ПРИВАТНОСТ БЕЗ „ЦУРЕЊА ПОДАТАКА”	104
МЕДИЈИ, ПЛАТФОРМЕ И ОДГОВОРНОСТ ЗА АЛГОРИТАМСКО ПОСРЕДОВАЊЕ	104
ГРАНИЦЕ АЛГОРИТАМСКЕ ОБРАДЕ: ПРАВО, ТРАНСПАРЕНТНОСТ И ОДГОВОРНОСТ	106
ДА ЛИ ГРАЂАНИН ЗАИСТА КОНТРОЛИШЕ СВОЈЕ ПОДАТКЕ?	107
ЗАКЉУЧАК	108
РЕФЕРЕНЦЕ	109
МЕДИЈСКА ПИСМЕНОСТ И СВЕСТ ГРАЂАНА СРБИЈЕ О	
ЗАШТИТИ ПРИВАТНОСТИ У ДИГИТАЛНОМ ОКРУЖЕЊУ:	
АНАЛИЗА ДОСТУПНИХ ПОКАЗАТЕЉА	110
УВОД	111
МЕДИЈСКА ПИСМЕНОСТ КАО КОМПЕТЕНЦИЈА САВРЕМЕНОГ ГРАЂАНИНА	112
ПРИВАТНОСТ И ПОДАЦИ О ЛИЧНОСТИ У ДИГИТАЛНОМ МЕДИЈСКОМ ОКРУЖЕЊУ	114
ПРАВНИ И ИНСТИТУЦИОНАЛНИ ОКВИР ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ У	
РЕПУБЛИЦИ СРБИЈИ	116
ПОКАЗАТЕЉИ СВЕСТИ ГРАЂАНА СРБИЈЕ О ЗАШТИТИ ПРИВАТНОСТИ	118
Забринутост грађана и процена ризика	119
Препознавање повреда приватности	120
Практичне способности заштите приватности	120
Познавање права и институционалних механизма	121
Разлика између ставова и понашања	121
УЛОГА МЕДИЈСКЕ ПИСМЕНОСТИ У УНАПРЕЂЕЊУ ЗАШТИТЕ ПРИВАТНОСТИ	122
ПРЕПОРУКЕ ЗА УНАПРЕЂЕЊЕ СВЕСТИ ГРАЂАНА О ЗАШТИТИ ПРИВАТНОСТИ	124
ЗАКЉУЧАК	125
РЕФЕРЕНЦЕ	126

МЕНАѢЕРСКЕ КОМПЕТЕНЦИЈЕ У УСЛОВИМА ПРИМЕНЕ	
ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ЗАШТИТЕ ПРИВАТНОСТИ	128
УВОД	129
МЕНАѢЕРСКЕ КОМПЕТЕНЦИЈЕ У САВРЕМЕНОМ ПОСЛОВНОМ ОКРУЖЕЊУ	130
ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА У САВРЕМЕНОЈ МЕНАѢЕРСКОЈ ПРАКСИ	134
ТРАНСФОРМАЦИЈА МЕНАѢЕРСКИХ КОМПЕТЕНЦИЈА У УСЛОВИМА ПРИМЕНЕ	
ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ	136
ЗАШТИТА ПРИВАТНОСТИ И ЕТИЧКА ОДГОВОРНОСТ МЕНАѢЕРА У	
ПРИМЕНИ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ	138
ЗАКЉУЧАК	139
РЕФЕРЕНЦЕ	140
МЕДИЈСКА ПИСМЕНОСТ И СВЕСТ ГРАЂАНА О ЗАШТИТИ ПРИВАТНОСТИ –	
РАЗЛИКЕ ИЗМЕЂУ ГЕНЕРАЦИЈА И НИВОА ОБРАЗОВАЊА	141
УВОД	142
ПОЈАМ МЕДИЈСКЕ ПИСМЕНОСТИ У САВРЕМЕНОМ ДИГИТАЛНОМ ОКРУЖЕЊУ	142
ПРИВАТНОСТ КАО САСТАВНИ ДЕО МЕДИЈСКЕ И ДИГИТАЛНЕ ПИСМЕНОСТИ	143
МЕТОДОЛОШКИ ПРИСТУП И ИЗВОРИ ПОДАТАКА	144
СТАЊЕ МЕДИЈСКЕ ПИСМЕНОСТИ У СРБИЈИ	145
СВЕСТ ГРАЂАНА О ЗАШТИТИ ПРИВАТНОСТИ	146
ГЕНЕРАЦИЈСКЕ РАЗЛИКЕ У МЕДИЈСКИМ НАВИКАМА И КРИТИЧКИМ	
КОМПЕТЕНЦИЈАМА	146
НИВО ОБРАЗОВАЊА КАО ФАКТОР МЕДИЈСКЕ И ДИГИТАЛНЕ ПИСМЕНОСТИ	147
УКРШТАЊЕ ГЕНЕРАЦИЈЕ И ОБРАЗОВАЊА	148
Млади са вишим нивоом образовања	148
Млади са нижим нивоом образовања	149
Средње генерације	149
Старији са вишим и високим образовањем	149
Старији са нижим образовањем	150
ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА КАО НОВИ ТЕСТ МЕДИЈСКЕ И	
ПРИВАТНОСНЕ ПИСМЕНОСТИ	150
ДИСКУСИЈА	151
ПРЕПОРУКЕ	151
ЗАКЉУЧАК	152
РЕФЕРЕНЦЕ	153
САЈБЕР БЕЗБЕДНОСТ КАО ИЗАЗОВ САВРЕМЕНОГ МЕНАѢМЕНТА У	
УСЛОВИМА ДИГИТАЛНЕ ТРАНСФОРМАЦИЈЕ	155
УВОД	156
ДИГИТАЛНА ТРАНСФОРМАЦИЈА КАО ОКВИР САВРЕМЕНОГ ПОСЛОВАЊА	157
САЈБЕР БЕЗБЕДНОСТ И РИЗИЦИ У ДИГИТАЛНОМ ПОСЛОВНОМ ОКРУЖЕЊУ	160
МЕНАѢМЕНТ САЈБЕР БЕЗБЕДНОСТИ У САВРЕМЕНИМ ОРГАНИЗАЦИЈАМА	162
МЕНАѢЕРСКЕ КОМПЕТЕНЦИЈЕ, ОРГАНИЗАЦИОНА КУЛТУРА И УПРАВЉАЊЕ	
САЈБЕР РИЗИЦИМА	164
ЗАКЉУЧАК	166
РЕФЕРЕНЦЕ	167
ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА, АЛГОРИТМИ И ПРИВАТНОСТ ГРАЂАНА	168
УВОД	169
ТЕОРИЈСКИ ДЕО	170
Вештачка интелигенција у савременом дигиталном окружењу	170
Алгоритми, аутоматизована обрада података и алгоритамско профилисање	171
Право на приватност и заштита личних података	172
Вештачка интелигенција, медији и друштвене мреже	170
Примена вештачке интелигенције у образовању и ризици по приватност	173
Етички и правни изазови примене вештачке интелигенције	174
МЕТОДОЛОГИЈА	174
ДИСКУСИЈА	175
ЗАКЉУЧАК	177
РЕФЕРЕНЦЕ	178

Уводна реч уредника

Поштовани читаоци,

Пред вама је специјални број Карловачког листа 021 под називом „Медији и заштита приватности у дигиталном добу: импликације за људска права и сигурност података“, посвећен једној од најактуелнијих и најзначајнијих тема савременог друштва. У времену у којем дигиталне технологије обликују готово сваки аспект људског живота, питања приватности, безбедности података и заштите основних људских права добијају посебан значај и захтевају континуирану научну, стручну и друштвену пажњу.

Савремени медијски екосистем карактеришу брзина преноса информација, глобална повезаност и све већа примена вештачке интелигенције, алгоритамског профилисања и аутоматизоване обраде података. Иако ове технологије отварају нове могућности за комуникацију, информисање и друштвени развој, истовремено постављају бројне изазове у погледу заштите приватности појединаца, безбедности дигиталног простора и очувања демократских вредности.

Полазећи од потребе да се ова питања сагледају из различитих научних и професионалних перспектива, окупили смо 14 аутора – истраживача, новинара, медијских стручњака – који су својим радовима дали драгоцен допринос разумевању сложених односа између медија, технологије, права и етике. Њихови текстови анализирају бројне аспекте дигиталне приватности: од права на заштиту личних података и медијске одговорности, преко улоге друштвених мрежа и сајбер безбедности, до изазова које доносе велики подаци и системи засновани на вештачкој интелигенцији.

Посебна вредност овог издања огледа се у мултидисциплинарном приступу који омогућава свеобухватније разумевање савремених процеса и подстиче дијалог између научне заједнице, медијских професионалаца, доносилаца одлука и шире јавности. Уверени смо да ће представљени радови допринети развоју критичког промишљања о дигиталним правима и одговорном коришћењу технологија, као и јачању свести о значају заштите приватности у савременом друштву.

Захваљујем свим ауторима на учешћу, члановима Издавачког савета на стручној подршци и свима који су допринели реализацији овог специјалног броја. Надам се да ће ова публикација представљати подстицај за нова истраживања, стручне расправе и конкретне активности усмерене ка изградњи сигурнијег, праведнијег и одговорнијег дигиталног окружења.

С поштовањем,

Уредник Карловачког листа 021
Проф. др Бранислав Санчанин

УТИЦАЈ МЕДИЈСКЕ ПИСМЕНОСТИ НА ПЕРЦЕПЦИЈУ РИЗИКА И ЗАШТИТУ ПРИВАТНОСТИ ГРАЂАНА

Бранислав Санчанин¹

Сажетак

Истраживачке активности које се баве приватношћу појединаца у онлајн простору указују на недостатак емпиријских доказа о томе на који начин медијска писменост утиче на перцепцију ризика и на понашање у вези са заштитом приватности. У том смислу циљ ове студије је испитивање динамичне мултилатералне везе између медијске писмености, активности у виртуелном простору, перцепције ризика и заштите приватности грађана. Чланак настоји да допринесе постојећем корпусу истраживања о приватности у онлајн окружењу, анализирајући реалне ризике које дигитални трагови корисника представљају по њихову приватност, као и да кроз теоријски оквир унапреди разумевање механизма заштите у савременом, динамичном и константно променљивом виртуелном простору. Наглашава се значај континуираног развоја медијске писмености као кључног предуслова за јачање свести о заштити приватности, али и за формулисање и спровођење ефикасних јавних политика усмерених ка заштити права корисника. Такође, указује се на потребу даљих емпиријских и теоријских истраживања ради дубљег и свеобухватнијег разумевања утицаја друштвених медија на приватност, као и идентификације проактивних стратегија које могу допринети унапређењу заштите корисника у дигиталном окружењу.

Кључне речи: медијска писменост, дигитални медији, приватност, перцепција ризика, заштита права корисника

¹ Универзитет „Унион – Никола Тесла”, Београд, Србија
e-mail: sancanin.branislav@gmail.com

УВОД

Савремени модели приватности у дигиталном простору заснивају се на претпоставци да појединци сnose примарну одговорност за заштиту својих података и ублажавање последица њиховог евентуалног нарушавања. Ипак, Reilly (2021) указује да обим и интензитет масовног прикупљања података суштински ограничавају капацитет појединаца да самостално управљају приватношћу и безбедношћу, отежавајући прецизно сагледавање и процену ризика који произлазе из њиховог присуства и активности у дигиталном окружењу. Интензиван развој медијског окружења довео је до повећане изложености приватности појединаца различитим облицима угрожавања, укључујући преваре, неовлашћено прикупљање и злоупотребу личних података. Иако приватност заузима значајно место у правним, религијским и друштвеним нормативним оквирима, недовољна развијеност медијске писмености често ограничава способност појединаца да препознају и ублаже ризике у дигиталном простору. У том контексту, унапређење регулаторних механизма, систематско јачање медијске писмености и развој дигиталних компетенција представљају кључне претпоставке за ефикасну заштиту приватности (Farzad, & Faridzadeh, 2025).

Све израженији тржишно оријентисан приступ посматра приватност као робу која се у дигиталном окружењу може размењивати за различите производе, услуге или погодности, при чему се занемарују нормативни и етички оквири на којима почива заштита основних људских права. Таква перспектива маргинализује значај законодавне регулативе и одговорности актера у дигиталном простору, пребацујући терет заштите приватности готово искључиво на појединца.

Перцепција приватности код људи првенствено се може усмерити на њих саме или на вредности приватности за друштво. Слично томе, заштита приватности може одбити индивидуалне и колективне претње приватности, видљиве кроз перципирану колективну вредност приватности током времена (Meier & Krämer, 2024). У том контексту, управљање дигиталним траговима, остваривање права на заборав, као и континуирана едукација, информисање и оснаживање грађана представљају кључне механизме за развој свести о облицима надзора и праћења у дигиталном окружењу. Истовремено, ове активности доприносе јачању капацитета појединаца да активно штите своја права и одбаце улогу пасивних, недовољно информисаних и обесправљених корисника дигиталних технологија.

Пораст онлајн активности у савременом дигиталном окружењу довео је до повећане забринутости за приватност и вези са безбедношћу. У том смислу Elrayah и Jamil (2023) истичу неопходност процене и истраживања дигиталних података ради утврђивања њихове веродостојности и валидности.

Упркос израженим изазовима и јасно уоченој забринутости корисника у вези са откривањем личних података, пракса дељења личних и туђих података у онлајн окружењу и даље је присутна. Trepte и сарадници (2015) развили су Скалу писмености о приватности на мрежи, која обухвата пет међусобно повезаних димензија: (1) знање о праксама организација, институција и пружалаца онлајн услуга; (2) разумевање техничких аспеката приватности и заштите података у дигиталном окружењу; (3) познавање законских и правних оквира заштите података на интернету; (4) упознатост са европским директивама у области приватности и заштите података; и (5) знање о стратегијама које корисници примењују у регулисању сопствене приватности.

Перцепција ризика и заштита приватности, уз хиперизложеност информацијама, као и фактори попут стреса, умора или преласка на друге платформе, могу представљати значајне детерминанте корективног понашања и саморегулације корисника, што се може манифестовати кроз редукцију или потпун престанак коришћења друштвених медија.

ПРЕГЛЕД ЛИТЕРАТУРЕ

Prince и сарадници (2024) истичу да корисници који примењују самозаштитне стратегије ради јачања заштите својих личних података имају тенденцију да перципирају виши ниво контроле над сопственим подацима. Резултати студије додатно указују на потребу за интензивирањем образовних активности усмерених на подизање свести корисника о њиховим правима и механизмима заштите података.

Bajnaid и Aljasir (2025) указују да су корисници у региону Блиског истока и Северне Африке у стању да донесу боље процене о својим онлајн изборима када разумеју везу између писмености о приватности на мрежи и заштите приватности, позивајући на опрез приликом генерализације резултата на друге популације. Такође, аутори нуде својеврсни путоказ програмерима за изградњу корисничких интерфејса који омогућавају корисницима да донесу информисане одлуке у вези са својом онлајн приватношћу.

Корпорације у све већој мери настоје да изграде прецизне алгоритамске профиле својих корисника ради различитих циљева, укључујући, између осталог, персонализацију оглашивачких садржаја. У том контексту, Zhang и сарадници (2024) излажу испитанике њиховим личним алгоритамским профилима како би испитали однос између перципиране тачности таквог профилисања, осећаја надзора и накнадних стратегија суочавања. Резултати указују на то да виши степен перципиране прецизности алгоритамских профила корелира са интензивнијим доживљајем надзора. Притом, појединци са нижим нивоом дигиталне писмености у домену заштите приватности показују израженију забринутост за приватност независно од перципираног надзора, док они са вишим нивоом такве писмености чешће развијају забринутост као последицу појачаног осећаја да су надзирани. Wang (2025) констатује да медијски алгоритам прожима сваку карку вести, од производње до дистрибуције, и анализира механизам рада медијских алгоритама, као и заштиту приватности корисника у дигиталном добу. Износе се конкретни предлози из три перспективе: регулаторна тела треба да уведу прописе и ојачају надзор; платформе треба да побољшају транспарентност алгоритама и да се придржавају „принципа минимално неопходног” у прикупљању информација; корисници треба да побољшају своју писменост о приватности и способност перцепције ризика.

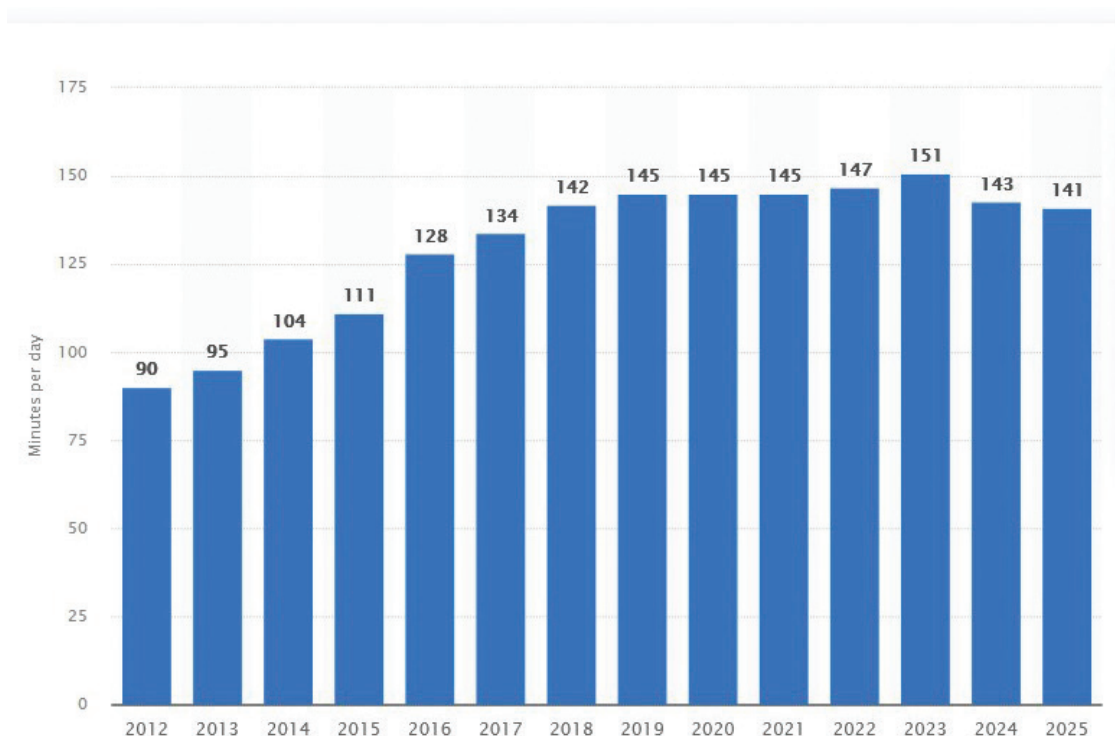
Yu и сарадници (2025) у својој студији показују да искуства са приватношћу, писменост о приватности и замор од приватности позитивно корелирају са понашањима усмереним на заштиту приватности. Такође, утврђено је да забринутост за приватност и претходна искуства са приватношћу позитивно утичу на појаву замора од приватности, док је писменост о приватности са њим негативно повезана. Даље, резултати указују да замор од приватности у потпуности посредује између забринутости за приватност и заштите приватности. Насупрот томе, његова медијаторска улога је делимична у односу између искустава са приватношћу и заштитног понашања, као и између писмености о приватности и заштите приватности.

Shrestha и сарадници (2024) анализирају однос између забринутости у вези са приватношћу, равнотеже између приватности и корисности, факторе поверења у вештачку интелигенцију, очекивања транспарентности и стратегије за побољшање контроле корисника над личним подацима. Налази откривају значајну забринутост у вези са приватношћу међу младим корисницима, укључујући перципирани недостатак контроле над личним подацима, потенцијалну злоупотребу података од стране вештачке интелигенције и страх од кршења

података и неовлашћеног приступа. Ова питања погоршавају нејасне праксе прикупљања података и недовољна транспарентност у апликацијама вештачке интелигенције. Намера дељења података је уско повезана са перципираним користима и гаранцијама заштите података. И поред континуираног компромиса између функционалних предности апликација заснованих на вештачкој интелигенцији и очувања приватности, корисници показују висок ниво свести о потенцијалним ризицима по приватност. Поверење у вештачку интелигенцију је под утицајем транспарентности, поузданости, предвидивог понашања и јасне комуникације о коришћењу података. У студији се истиче потреба свеобухватног образовања о приватности података.

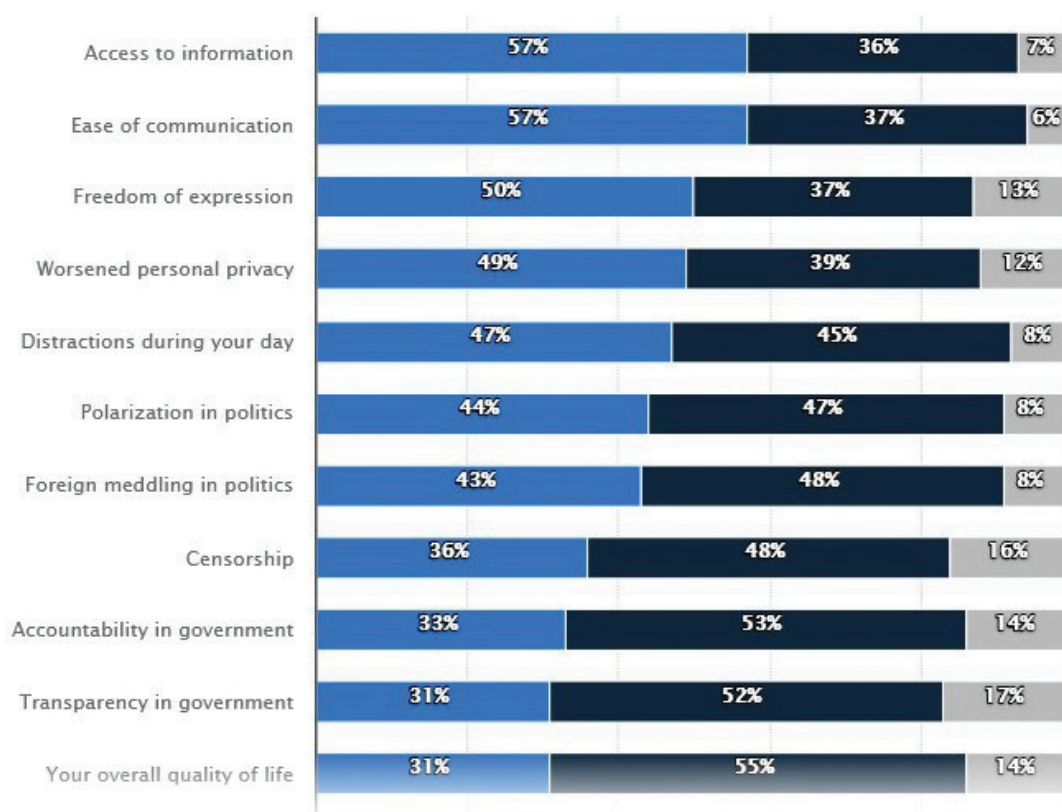
ЗАШТИТА ПРИВАТНОСТИ КОРИСНИКА НА ДРУШТВЕНИМ МРЕЖАМА

Друштвени медији карактеришу изузетно широк домет и глобална распрострањеност. Употреба онлајн мрежа континуирано расте паралелно са експанзијом дигиталне популације, при чему су корисници интернета током 2025. године у просеку проводили око 141 минут дневно на друштвеним платформама. Земља у којој корисници дневно проводе највише времена на друштвеним мрежама је Бразил, у просеку 3 сата и 49 минута, док је дневно време provedено на друштвеним мрежама у САД 2 сата и 16 минута (Thuy, 2026).



Слика 1. Дневно provedено време на друштвеним мрежама корисника интернета широм света од 2012. до 2025. године
Извор: Thuy, 2026

Процене указују да је у 2025. години више од 5,4 милијарде људи широм света активно користило друштвене медије. Домет друштвених медија је широк: коришћење онлајн мрежа шири се заједно с глобалном дигиталном популацијом, а корисници интернета су 2025. године у просеку проводили 141 минут дневно на друштвеним платформама. Утицај друштвених медија обухвата широк спектар аспеката друштвеног живота, при чему се њихове последице не ограничавају искључиво на онлајн окружење, већ се рефлектују и на понашање појединаца у свакодневним активностима. Налази глобалног истраживања спроведеног међу корисницима интернета у фебруару 2019. године указују да су испитаници друштвеним медијима приписали значајан допринос већој доступности информација, ефикаснијој комуникацији и већој слободи изражавања. Истовремено, перцепција њихових негативних ефеката огледа се у оцени да доприносе нарушавању личне приватности, јачању политичке поларизације и повећању свакодневних ометајућих садржаја и активности. (Slotta, 2026).



Слика 2. Удео корисника интернета широм света који верују да су платформе друштвених медија имале утицај на одабране аспекте свакодневног живота од фебруара 2019. године

Извор: Slotta, 2026

Регулаторни приступ Европске уније заснива се на строгој заштити личних података и контроли садржаја који може угрозити права и безбедност корисника дигиталних платформи. Друштвене мреже и друге технолошке компаније подлежу обавезујућим правилима и прописима које је усвојио Европски парламент, а њихово непоштовање може довести до изрицања високих новчаних казни. Посебна пажња посвећује се заштити малолетних корисника, која представља један од приоритетних циљева савремене европске дигиталне регулативе (European Union, 2016; European Union, 2022).

Правни оквир Републике Србије не садржи посебан закон којим се уређује заштита приватности корисника друштвених медија. Заштита се остварује применом општих прописа, првенствено Закона о заштити података о личности, Закона о електронским комуникацијама, Устава Републике Србије и релевантних одредаба Кривичног законика. За разлику од Европске уније, која је усвојила посебне регулаторне инструменте попут DSA и DMA, српски регулаторни оквир још увек не познаје свеобухватну регулацију која би била усмерена искључиво на заштиту корисника дигиталних платформи и друштвених медија.

Базични пропис за заштиту података у дигиталном простору је Закон о заштити података о личности (2018), који уређује обраду података о личности, пристанак корисника и његова права, као на пример право на приступ, исправку, брисање, ограничење обраде и пренос података, затим обавезе компанија које обрађују податке, пренос података у иностранство, надзор и санкције.

Устав Републике Србије (2006) у члану 42 гарантује заштиту података о личности као једно од основних људских права и прописује да се прикупљање, обрада и коришћење података уређује законом.

„Зајемчена је заштита података о личности. Прикупљање, држање, обрада и коришћење података о личности уређују се законом. Забрањена је и кажњива употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом. Свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом, и право на судску заштиту због њихове злоупотребе.”

Закон о електронским комуникацијама Републике Србије (2023) нормира битне аспекте заштите приватности корисника у дигиталном окружењу, посебно у погледу тајности комуникација и обраде података. Закон прописује обавезу пружалаца услуга да обезбеде тајност електронских комуникација и са њима повезаних саобраћајних података, укључујући садржај комуникације. Обрада података о саобраћају ограничена је на строго дефинисане сврхе, као што су наплата услуга, управљање мрежом и техничко обезбеђивање функционалности система, док је за друге облике обраде, укључујући комерцијалне сврхе, неопходан пристанак корисника. Додатно, уведена је посебна заштита података о локацији корисника, омогућавајући њихову обраду искључиво уз анонимизацију или претходну сагласност корисника. Прописана је и обавеза примене одговарајућих техничких и организационих мера ради заштите задржаних података од неовлашћеног приступа, измене или злоупотребе. Мада се термин „колачићи” експлицитно не наводи у законском тексту, њихова примена се посредно уређује кроз режим пристајка корисника и опште одредбе о обради података о личности.

Кривични законик Републике Србије (2005) предвиђа кривична дела која могу да буду повезана са повредом приватности, као што су неовлашћено прикупљање личних података, фотографисање, прислушкивање и снимање, као и угрожавање сигурности или прогањање путем информационо-комуникационих технологија.

Надзор је поверен Поверенику за информације од јавног значаја и заштиту података о личности, којем грађани могу поднети притужбу уколико сматрају да су њихови подаци на друштвеним мрежама или другим интернет сервисима незаконито обрађени.

ЗАКЉУЧАК

Бројна емпиријска истраживања указују на то да корисници са нижим нивоом писмености у области заштите приватности имају отежане капацитете за адекватну процену ризика којима су изложени. Овакав налаз је очекиван, с обзиром на то да виши нивои писмености корелирају са развијенијим способностима критичке интерпретације и евалуације информација. На основу тога може се закључити да критичко разумевање информација функционише као кључни механизам заштите, омогућавајући ефикасније управљање понашањем дигиталних корисника и ублажавање ризика повезаних са нарушавањем приватности. Ови налази упућују на потребу за систематском и континуираном едукацијом, како би корисници развили способност прецизнијег вредновања потенцијалних претњи по приватност. Осим тога, резултати имају значајне импликације за различите актере у дигиталном окружењу, док самим корисницима омогућавају доношење информисаних одлука о обиму и границама дељења личних података. Упркос континуираном успостављању равнотеже између заштите приватности и функционалних користи које пружају апликације засноване на вештачкој интелигенцији, корисници исказују висок степен опреза према потенцијалним ризицима по приватност. Као основни предуслови за прихватање ових технологија издвајају се транспарентност у обради података, могућност приступа, исправке и контроле личних података, поуздане гаранције њихове заштите, као и јасно дефинисани механизми давања информисане сагласности.

РЕФЕРЕНЦЕ

Bajnaid, W., & Aljasir, S. (2025). Does Online Privacy Literacy Affect Privacy Protection Behaviour? A Mixed-Methods Study of Digital Media Users in the MENA Region. *Journalism and Media*, 6(1), 8. <https://doi.org/10.3390/journalmedia6010008>

Elrayah, M. & Jamil, S. (2023). Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness. *International Journal of Cyber Criminology*, 17(2), 166-187. <https://doi.org/10.5281/zenodo.4766711>

European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR). Доступно на: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> (Приступљено: 20. јун 2026.)

European Union. (2022). Regulation (EU) 2022/2065 (Digital Services Act – DSA). Доступно на: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065> (Приступљено: 20. јун 2026.)

Farzad, E., & Faridzadeh, M. (2025). Protecting the privacy of users in the digital world; the vital role of media literacy. *Jurisprudence and legal studies of media*, 6(2), 337-368.

Кривични законик Републике Србије (2005). Службени гласник Републике Србије, 85/2005-испр., 107/2005-испр., 72/2009, 111/2009, 104/2013, 108/2014, 94/2016, 35/2019 и 04/2024,

Shrestha, A. K., Barthwal, A., Campbell, M., Shouli, A., Syed, S., Joshi, S., & Vassileva, J. (2024). Navigating AI to unpack youth privacy concerns: An in-depth exploration and systematic review. In

2024 IEEE 15th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (116–123). IEEE.

<https://doi.org/10.1109/IEMCON62851.2024.11093125>

Meier, Y., & Krämer, N. C. (2024). A longitudinal examination of Internet users' privacy protection behaviors in relation to their perceived collective value of privacy and individual privacy concerns. *New Media & Society*, 26(10), 5942–5961.

<https://doi.org/10.1177/14614448221142799>

Prince, C., Omrani, N., Schiavone, F. (2024), Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe. *Information Technology & People*, 37(8), 1–24, <https://doi.org/10.1108/ITP-05-2023-0467>

Reilly, A. C. (2021). Reading risk: Preparing students to develop critical digital literacies and advocate for privacy in digital spaces. *Computers and Composition*, 61, 102652.

<https://doi.org/10.1016/j.compcom.102652>

Slotta, D. (2026). Social media - statistics & facts. Statista. Доступно на:

<https://www.statista.com/topics/1164/social-networks/#topicOverview> (Accessed: Jun 12, 2026)

Thuy, D. (2026). Average daily time spent on social media worldwide 2012–2025. Statista. Доступно на: <https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide> (Приступљено: 30. априла 2026.)

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In: Gutwirth, S., Leenes, R., de Hert, P. (Eds) *Reforming European Data Protection Law. Law, Governance and Technology Series*, 20. Springer, Dordrecht. https://doi.org/10.1007/978-94-017-9385-8_14

Устав Републике Србије (2006). Службени гласник Републике Србије, 98/2006, 115/2021.

Wang, M. (2025). Media Algorithms and User Privacy Protection: a Dynamic Game of Conflict and Balance. *Procedia Computer Science*, 261, 605–611.

<https://doi.org/10.1016/j.procs.2025.04.251>

Yu, X., Sun, J., & Zhang, X. (2025). Privacy-related factors on social media users' privacy protection behaviors: an APFO model perspective. *Online Information Review*, 49(5), 991–1006. <https://doi.org/10.1108/OIR-08-2024-0530>

Закон о заштити података о личности (2018). Службени гласник Републике Србије, 87/2018.

Закон о електронским медијима Републике Србије (2023). Службени гласник Републике Србије, 35/2023.

Zhang, D., Strycharz, J., Boerman, S.C., Araujo, T., Voorveld, H., (2024). Google knows me too well! Coping with perceived surveillance in an algorithmic profiling context. *Computers in Human Behavior*, 165, 108536. <https://10.1016/j.chb.2024.108536>

УТИЦАЈ ДРУШТВЕНИХ МЕДИЈА НА МЕНТАЛНО ЗДРАВЉЕ МЛАДИХ: МУЛТИДИМЕНЗИОНАЛНИ ПРИСТУП

Александра Пењишевић¹

Сажетак

Упркос значајном корпусу спроведених истраживања, налазима који се односе на сложен и вишеслојан утицај друштвених медија на здравље младих и даље доминира висок степен неуједначености, при чему се у литератури често сусрећу супротстављени, па чак и дијаметрално опречни закључци у погледу њихових позитивних и негативних ефеката. Ова хетерогеност резултата указује на чињеницу да мултидимензионална природа односа између коришћења друштвених медија и здравља младих у великој мери остаје недовољно теоријски и емпиријски разјашњена, нарочито када је реч о контекстуалним факторима који условљавају начине употребе, као и о импликацијама које такви обрасци коришћења имају на понашања у дигиталном, односно виртуелном окружењу. Полазећи од наведених теоријских и емпиријских недоумица, основни циљ ове студије јесте систематска анализа постојећих научних доказа о ефектима употребе друштвених медија на ментално здравље младих, уз истовремено настојање да се идентификују кључне празнине у тренутном знању, као и да се назначе правци и потенцијали за будућа истраживања у овој области. Посебан фокус усмерен је на потребу за дубљим разумевањем механизма путем којих различити обрасци коришћења друштвених медија генеришу дивергентне исходе по ментално здравље. У том контексту, ефикасно ублажавање потенцијалних здравствених ризика повезаних са употребом друштвених медија код младих, уз паралелно препознавање, афирмацију и оптимално искоришћавање њихових позитивних аспеката, могуће је остварити искључиво кроз дугорочно, систематично и интердисциплинарно унапређење медијске писмености. Осим тога, од значаја је и развој инклузивног, сигурног и подржавајућег дигиталног окружења које подстиче одговорно коришћење технологије и оснажује младе за критичко промишљање и конструктивно учешће у савременом медијском простору.

Кључне речи: друштвени медији, медијска писменост, инфодемија, ментално здравље, здравствени ризици

¹ Универзитет „Унион – Никола Тесла”, Београд, Србија
e-mail: aleksandra.penjisevic@gmail.com

УВОД

Друштвени медији обилују приликама за социјална поређења, због чега истраживање ефеката како краткотрајне, тако и дуготрајне изложености садржајима релевантним за социјално поређење представља трајну истраживачку потребу. Резултати емпиријских студија указују на то да је учестала употреба друштвених мрежа повезана са нижим нивоом самопоштовања у домену личних карактеристика. На пример, утврђено је да корисници Фејсбука чешће исказују смањено самопоуздање, при чему је овај однос посредован повећаном изложеношћу процесима социјалног поређења. Такође, експериментална истраживања привремене изложености профилима на друштвеним мрежама показују да су самопоштовање и релативне самопроцене учесника биле ниже када су профили циљне особе садржали елементе неповољних поређења, као што су нижи ниво друштвене активности или присуство нездравих животних навика (Vogel et al., 2014). Посебно забрињава и опомиње чињеница да се доминантан део процена о штетном утицају друштвених мрежа на младе и даље ослања на субјективне исказе прикупљене кроз упитнике самопроцене, док је занемарљиво мали број истраживања који ове налазе поткрепљује клинички објективнијим индикаторима, на пример симптомима менталних поремећаја.

Битан теоријски став јесте онај који истиче да кључна детерминанта валенције изложености младих утицајима друштвених медија, као и односа између потенцијалних ризика и користи, није временски обим коришћења, већ квалитативна природа интеракције са тим медијима. (Davila et al., 2012; Feinstein et al., 2013.)

Позитивне импликације употребе друштвених медија на младе Lioyd (2014) сажима у неколи сегмената, а посебно истиче позитивне рефлексije на младе у мањинским заједницама, особама са инвалидитетом или особе са хроничним боестима, с обзиром на пружену могућност повезивања са другима који живе сличним животима упркос географског удаљености. Указује се на то да би креатори политика и здравствени радници могли да користе друштвене медије ради повезивања по питању менталног здравља.

Медијска хиперпродукција довела је до експоненцијалног раста количине информација које циркулишу у дигиталном простору, међу којима значајно место заузимају дезинформације, нетачно интерпретирани садржаји и непроверене гласине. Окрау (2022) указује на налазе према којима је феномен инфодемије повезан са порастом учесталости различитих поремећаја менталног здравља, укључујући деперсонализацију и дереализацију, анксиозност, депресију, као и суицидалне идеације. Овакви трендови носе потенцијално озбиљне друштвене импликације, будући да нарушавају способност појединаца да доносе рационалне и научно утемељене одлуке. Поред тога, запажена је и трансформација дискурских образаца унутар онлајн заједница за подршку особама са менталним поремећајима, при чему долази до израженог пораста садржаја обележених негативним афективним стањима, попут безнађа, беспомоћности, усамљености, па чак и темама везаним за самоубиство.

Значајан број људи са менталним болестима не користи услуге менталног здравља да би добили лечење. Данас постоје убедљиви докази да особе са менталним и психосоцијалним тегобама имају све већу свест и траже све већи утицај и контролу над догађајима у својим животима и над третманима. У том контексту, друштвени медији тј. мејлови, видео позиви, текстуалне поруке, линије за разговор и друштвене мреже, појавили су се током година на позадини експоненцијалног раста. Ширење редизајнираних технологија може омогућити услуге усмерене ка пацијенту, стратегије за оснаживање пацијената и персонализацију неге, заједно са смањењем трошкова. Такође, расте интересовање за примену друштвених медија у заштити менталног здравља (Di Napoli et al., 2015).

ДРУШТВЕНЕ МРЕЖЕ: ПОЗИТИВНЕ ИМПЛИКАЦИЈЕ НАСУПРОТ НЕГАТИВНИХ ИМПЛИКАЦИЈА

Друштвене мреже представљају интегрални сегмент свакодневног живота тинејџера. Међутим, њихова све већа заступљеност истовремено генерише забринутост у погледу потенцијалних негативних импликација. Савремена истраживања, као и ставови родитеља, указују на то да континуирана дигитална повезаност, пролонгирано коришћење друштвених мрежа у касним вечерњим сатима, те притисци инхерентни онлајн интеракцијама, могу имати неповољан утицај на психолошку добробит младих, њихов академски учинак, као и укупно здравствено стање (Richter, 2026).

Истражујући емоционална искуства млађих корисника у контексту коришћења друштвених мрежа, Christodoulou et al. (2026) идентификују три кључна тематска правца. Прво, аутори разматрају емоционалне последице употребе друштвених медија, укључујући феномене дистанцирања и повремених прекида коришћења као стратегије суочавања са осећајем исцрпљености, замора и психолошког оптерећења. Друго, истиче се растуће неповерење према друштвеним платформама и онлајн информативним садржајима, које се манифестује кроз појачан скептицизам према дезинформацијама, алгоритамски посредованим садржајима и савременим технологијама вештачке интелигенције. Треће, анализирана је присутност агресивних образаца комуникације на мрежама, при чему корисници бивају изложени непријатељском дигиталном окружењу и развијају различите одбрамбене механизме ради његовог избегавања. Налази указују на динамичну трансформацију образаца понашања кроз време: ранији модели активног учешћа и дељења садржаја уступили су место израженијем опрезу, неповерењу и дистанци. Ова промена интерпретира се као покушај заштите од емоционалне исцрпљености и негативних последица изложености непоузданим или штетним информацијама. Док се постојећа литература доминантно фокусира на искуства млађих кохорти, предметна студија значајно доприноси области истраживања тиме што се усмерава на недовољно истражену популацију особа средњих година.

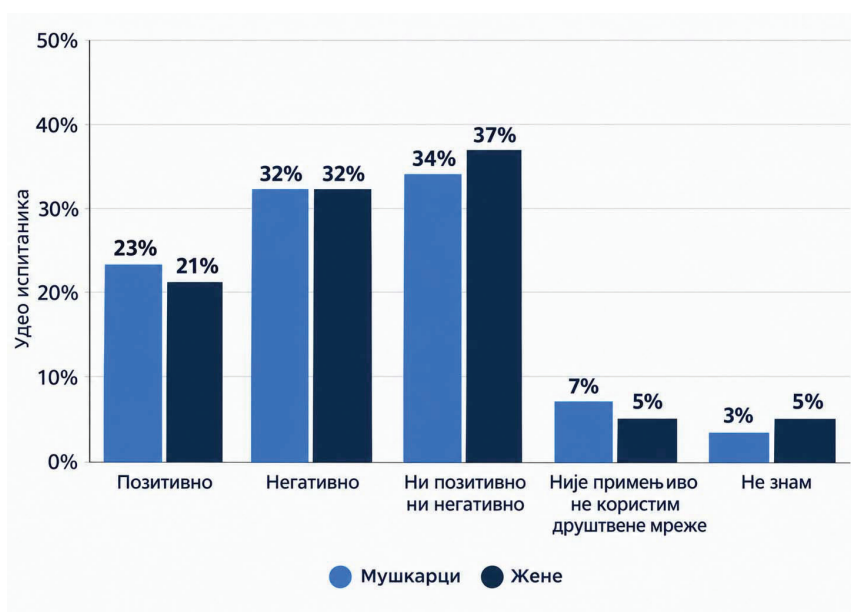
Када су Faverio et al (2025) из Истраживачког центра Пју испитали америчке тинејџере о потенцијалним ефектима друштвених мрежа, они су указали на њихову двосмерну природу: као извора користи и ризика. Поједини аспекти живота перципирани су као унапређени употребом друштвених мрежа, при чему је 30% тинејџера навело позитиван утицај на пријатељства, док је 19% истакло пораст самопоуздања, чинећи ове области јединима са претежно позитивним нето ефектом. Насупрот томе, негативни ефекти чешће се пријављују у доменима школског рада и свакодневног функционисања: 40% тинејџера сматра да друштвене мреже умањују њихову продуктивност (наспрам 9% који виде корист), док 22% верује да негативно утичу на школске оцене, у поређењу са свега 8% који наводе побољшање.

Најизраженији негативни утицај односи се на сан: чак 45% испитаника наводи да друштвене мреже смањују количину сна коју остварују, док само 4% сматра да доприносе квалитетнијем одмору. Ови резултати указују да је сан област која се перципира као највише нарушена, наглашавајући посебно неповољан ефекат касновечерњег коришћења друштвених мрежа на обрасце одмора младих.



Слика 1. Удео америчких тинејџера узраста од 13 до 17 година који кажу да користе друштвене мреже: много/мало (%)
Напомена: Анкета спроведена од 18. септембра до 10. октобра 2024.
Извор: Pew Research Center, 2025

Према истраживању спроведеном у Сједињеним Америчким Државама у децембру 2025. године, забележене су благе родне разлике у перцепцији утицаја друштвених мрежа на ментално здравље: 23% мушких испитаника и 21% женских испитаника оценило је овај утицај као позитиван. Истовремено, једнак удео од 32% испитаника оба пола навео је да друштвене мреже имају негативан ефекат на њихово ментално здравље.



Графикон 1. Утицај друштвених медија на ментално здравље одраслих у САД 2025. године, по полу
Извор: Statista Research Department, 2025.

Коришћење друштвених медија препознаје се као потенцијални фактор ризика за развој проблема у домену менталног здравља код адолесцентске популације. Ипак, упркос растућем интересовању научне заједнице за ову тему, број лонгитудиналних истраживања која систематски испитују ову повезаност и даље је ограничен, док ниједно од постојећих истраживања није прецизно квантификовало колики се удео проблема менталног здравља међу адолесцентима може директно приписати употреби друштвених медија.

У том контексту, Riehm и сарадници (2019) реализовали су лонгитудиналну кохортну студију која је обухватила узорак од 6.595 испитаника, праћених кроз три истраживачка таласа: први у периоду од 12. септембра 2013. до 14. децембра 2014. године, други од 23. октобра 2014. до 30. октобра 2015. године и трећи од 18. октобра 2015. до 23. октобра 2016. године. Резултати ове студије указују на то да адолесценти који проводе више од три сата дневно на друштвеним медијима могу бити изложени повећаном ризику од развоја проблема менталног здравља, при чему су нарочито изражени тзв. интернализовани проблеми, као што су анксиозност и депресивност. На основу ових налаза, аутори наглашавају потребу за даљим истраживањима која би систематски испитала ефикасност различитих интервенцијских стратегија. Конкретно, предлаже се да будуће студије размотре да ли увођење ограничења у свакодневном трајању коришћења друштвених медија, унапређење нивоа медијске писмености, као и потенцијални редизајн самих платформи друштвених медија, могу представљати делотворне приступе у смањењу оптерећења проблемима менталног здравља међу адолесцентима.

Аспект	Позитивне импликације	Негативне импликације	Референце
Депресија и анксиозност	Умерена употреба може допринети осећају припадности и друштвеној подршци.	Повећана преваленција депресивних и анксиозних симптома међу адолесцентима са високим нивоом коришћења друштвених медија.	Watson i sar., 2026 Tsomokos, 2025
Самопоштовање и слика о себи	Прилика за изражавање идентитета и добијање позитивних повратних информација од вршњака.	Негативни ефекти социјалног поређења, посебно међу адолесценткињама; повећан ризик од лоше слике тела.	Tsomokos, 2025
Спавање	Умерено ангажовање може смањити осећај изолације, чиме се индиректно побољшава квалитет сна.	Већа употреба је повезана са поремећајима спавања и краћим трајањем спавања.	Tsomokos, 2025
Когнитивне функције	Умерена употреба може подржати когнитивно ангажовање и приступ информацијама, потенцијално побољшавајући одређене процесе учења.	Прекомерна употреба је повезана са смањеним распоном пажње, оштећеном концентрацијом и потенцијалним негативним ефектима на извршне функције.	Watson i sar., 2026
Суицидалне идеје и понашања	Не постоје јасни лонгитудинални докази о заштитном ефекту.	Повећан ризик од суицидалних идеја и покушаја међу адолесцентима са стално високим или брзо растућим коришћењем друштвених медија.	Watson i sar., 2026

Табела 1. Утицај друштвених медија на ментално здравље младих: докази из лонгитудиналних студија

Извор: Аутори, на основу података из више извора (видети референце), 2026.

Према извештају U.S. Surgeon General's Advisory (2023), у Сједињеним Америчким Државама уочава се тренд опадања друштвене повезаности. У периоду од 2003. до 2020. године, време које појединци проводе у дружењу са пријатељима смањено је за приближно 20 сати месечно, док је друштвена интеракција са другим особама опала за око 10 сати месечно. Истовремено, особе које доживљавају усамљеност или су незадовољне квалитетом својих друштвених односа суочавају се са повећаним ризиком од превремене смртности, као и са неповољнијим здравственим исходима. Емпиријски налази указују да усамљеност значајно доприноси већем ризику од развоја анксиозности, депресије и деменције.



Слика 2. Три виталне компоненте друштвене повезаности
Извор: Holt-Lunstad, 2018

На основу лонгитудиналног истраживања спроведеног на национално репрезентативном узорку одраслих у Холандији, прикупљаног кроз девет годишњих таласа, Roberts и сарадници (2026) налазе да пасивно коришћење друштвених медија може допринети порасту усамљености. Истовремено, аутори истичу да је још увек преурањено закључити да активно коришћење друштвених медија има протективни ефекат у смислу смањења усамљености. Добијени резултати додатно указују на постојање двосмерне повезаности између нивоа коришћења друштвених медија и усамљености.

ЗАКЉУЧАК

Резултати ове студије доприносе повећаном разумевању механизма који посредују у односу између коришћења друштвених медија и неповољних исхода по ментално здравље. У том смислу, наглашава се потреба за континуираним истраживачким фокусом на детектовање и анализу специфичних процеса који произлазе из комплексних интеракција унутар виртуелног простора, а који могу бити здравствено забрињавајући. Упоредо са растом броја корисника друштвених медија, учесталије је незадовољство друштвеним интеракцијама, осећајем слабије повезаности са другим људима и све израженијом усамљеношћу. Перципирани осећај усамљености доводи чешће људе до ризика од анксиозности, депресије и деменције, као и неуролошких и кардиолошких обољења. У ширем контексту, намеће се потреба за развојем и имплементацијом циљаних интервенција усмерених на ублажавање и редукцију умора, психолошке исцрпљености и тескобе повезане са коришћењем друштвених медија. Важно је унапређивати компетенције корисника у препознавању дезинформација, као и јачати поверење у дигиталне платформе путем адекватних едукативних и регулативних стратегија. Будућа истраживања требало би да посвете знатно више пажње феномену негативног социјалног поређења током употребе друштвених мрежа, с обзиром на то да се овај процес доводи у везу са порастом депресивних симптома, као и суицидних идеја и покушаја међу млађом популацијом. Забрињава чињеница да се претежни део процена штетних ефеката употребе друштвених медија на младе заснива на подацима добијеним путем инструмената самопроцене, док је занемарљив број истраживања који се ослањају на објективније индикаторе, попут клинички релевантних симптома менталних поремећаја, што указује на значајно методолошко ограничење у постојећој емпиријској литератури.

РЕФЕРЕНЦЕ

Christodoulou, V., Konstantinou, P., Photiou, A., & Iordanou, K. (2026). Lost in the scroll: Emotional impacts of social media use among middle-aged adults. *Psychology of Popular Media*. <https://doi.org/10.1037/ppm0000671>

Davila, J., Hershenberg, R., Feinstein, B. A., Gorman, K., Bhatia, V., & Starr, L. R. (2012). Frequency and quality of social networking among young adults: Associations with depressive symptoms, rumination, and corumination. *Psychology of Popular Media Culture*, 1(2), 72–86. <https://doi.org/10.1037/a0027512>

Di Napoli, W.A., Nollo, G., Pace, N. i Torri, E. (2015). Can the Clinical Use of Social Media Improve the Quality of Care in Mental Health? A Health Technology Assessment Approach in an Italian Mental Health Service. *Psychiatria Danubina*, 27 (1), 103-110.

Faverio, M., Anderson, M., Park, E. (2025). Teens, Social Media and Mental Health. Доступно на: <https://www.pewresearch.org/internet/2025/04/22/teens-social-media-and-mental-health/#how-teens-see-social-media-s-impact-on-mental-health-friendships-sleep> (Приступљено: 22. маја 2026.)

Feinstein, B. A., Hershenberg, R., Bhatia, V., Latack, J. A., Meuwly, N., & Davila, J. (2013). Negative social comparison on Facebook and depressive symptoms: Rumination as a mechanism. *Psychology of Popular Media Culture*, 2(3), 161–170. <https://doi.org/10.1037/a0033111>

Holt-Lunstad, J. (2018). Why Social Relationships Are Important for Physical Health: A Systems Approach to Understanding and Modifying Risk and Protection. *Annual Review Psychology*, 69, 437–458. <https://doi.org/10.1146/annurev-psych-122216-011902>

Lloyd, A. (2014). Social Media: Help or Hindrance – What Role Does Social Media Play in Young People's Mental Health? *Psychiatria Danubina*, 26(1), 340–346.

Okray, Z. (2022). Infodemic and Mental Health Consequences. *Collegium antropologicum*, 46(1), 69–76. <https://doi.org/10.5671/ca.46.1.10>

Pew Research Center (2025). % of U.S. teens ages 13 to 17 who say using social media _ each of the following a lot/a little. Доступно на: https://www.pewresearch.org/internet/2025/04/22/teens-social-media-and-mental-health/pi_2025-04-22_teen-social-media-mental-health_0-10/ (Приступљено: 6. јуна 2026.)

Richter, F. (2026). Social Media Is Keeping Teens from a Good Night's Sleep. Доступно на: <https://www.statista.com/chart/35970/self-reported-effects-of-social-media-use-on-teenagers/?lid=pp5gj2rnpdwl> (Приступљено: 27. јуна 2026.)

Roberts, J. A., Young, P. D., & David, M. E. (2026). The Epidemic of Loneliness: A 9-Year Longitudinal Study of the Impact of Passive and Active Social Media Use on Loneliness. *Personality and Social Psychology Bulletin*, 52(5), 1111–1125.

Statista Research Department, (2025). Mental health effects of social media for adults in the U.S. 2025, by gender. Доступно на: <https://www.statista.com/statistics/1457452/effect-of-social-media-on-mental-health-gender/> (Приступљено: 15. јуна 2026.)

Tsomokos, D.I. (2025). Adolescent social media use and psychiatric outcomes: a longitudinal mediation analysis via interpersonal distrust, sleep, and self-image. *Social Psychiatry and Psychiatric Epidemiology*. <https://doi.org/10.1007/s00127-025-02999-w>

Vogel, E. A., Rose, J. P., Roberts, L. R., & Eckles, K. (2014). Social comparison, social media, and self-esteem. *Psychology of Popular Media Culture*, 3(4), 206–222. <https://doi.org/10.1037/ppm0000047>

Watson, C. S., Henrich, C. C., Long, D. M., & Fobian, A. D. (2026). Longitudinal Effects of Adolescent Digital Media Use on Mental Health in Young Adulthood. *Children*, 13(2), 215. <https://doi.org/10.3390/children13020215>

U.S. Surgeon General's Advisory. (2023). *Our epidemic of loneliness and isolation: The U.S. Surgeon General's Advisory on the healing effects of social connection and community*. Доступно на: <https://www.hhs.gov/sites/default/files/surgeon-general-social-connection-advisory.pdf> (Приступљено: 27. јуна 2026.)

АЛГОРИТАМСКА ПЕРСОНАЛИЗАЦИЈА И ЗАШТИТА ПРИВАТНОСТИ У ДИГИТАЛНИМ МЕДИЈИМА

Бојана Остојић¹

Сажетак

Савремени дигитални медији заснивају се на интензивној обради података, алгоритамској селекцији садржаја и све широј примени вештачке интелигенције. Такво окружење истовремено проширује приступ информацијама и отвара сложена питања заштите приватности, безбедности личних података и очувања аутономије корисника. Циљ рада је анализа кључних ризика који настају у процесу прикупљања, профилисања и коришћења података у дигиталним медијима, као и разматрање механизма којима се може успоставити равнотежа између права јавности на информисање, слободе изражавања и права појединца на приватност. Рад је теоријског и компаративног карактера и заснива се на анализи савремене научне литературе, европског регулаторног оквира и релевантних правила у Републици Србији. Посебна пажња посвећена је алгоритамском профилисању, персонализованом оглашавању, системима препорука, тзв. тамним обрасцима, генеративној вештачкој интелигенцији и deepfake садржајима. Анализа показује да се заштита приватности више не може свести само на формално прибављање пристанка, већ захтева примену принципа минимизације података, транспарентности, приватности по дизајну, корисничке контроле и континуиране процене ризика. У раду се предлаже модел одговорне дигиталне комуникације који повезује технолошку ефикасност са заштитом основних права и јачањем поверења у медије и дигиталне платформе.

Кључне речи: дигитални медији, приватност, лични подаци, алгоритми, профилисање, вештачка интелигенција, људска права.

¹ Бојана Остојић, Универзитет Едуконс, Факултет за пројектни и иновациони менаџмент Професор „Петар Јовановић”; e-mail bojanaostojic85@gmail.com

УВОД

Дигитални медији су током последње две деценије постали кључна инфраструктура свакодневног информисања, комуникације, забаве и друштвене интеракције. За разлику од традиционалног медијског система, у којем су уредничка селекција и институционална одговорност били релативно јасно препознатљиви, савремени дигитални простор функционише кроз сложену мрежу платформи, алгоритама, огласних система, мобилних апликација и услуга које непрекидно прикупљају и обрађују податке о понашању корисника. Корисник зато више није само публика: он истовремено представља извор података, предмет профилисања и циљ персонализоване комуникације.

Таква трансформација донела је бројне користи. Информације су доступне брже, јавна дебата је отворенија, а појединци имају могућност да непосредно учествују у креирању и дистрибуцији садржаја. Међутим, предности дигиталне комуникације прате ризици који се односе на неконтролисано прикупљање података, праћење активности, повезивање информација из различитих извора, алгоритамско профилисање, манипулативно усмеравање пажње и неовлашћени приступ осетљивим информацијама. Приватност је због тога постала једно од централних питања дигиталних права.

Проблем је нарочито сложен јер корисник често нема потпун увид у токове података који стоје иза наизглед једноставних активности у дигиталном окружењу. Отварање вести, задржавање на видео-снимку, претрага одређене теме или клик на оглас могу представљати сигнале који се повезују са претходним интеракцијама и користе за формирање профила, предвиђање интересовања и прилагођавање будућег садржаја. На тај начин дигитални медији више нису само канали за преношење информација, већ постају системи који активно обликују информационо окружење појединца. Gillespie (2014) указује да алгоритми нису неутрални технички инструменти, већ механизми који утичу на то који ће садржаји бити видљиви, релевантни и доступни кориснику. Истовремено, Zuboff (2015, 2019) овакву трансформацију корисничког искуства у податке погодне за анализу, предвиђање и комерцијалну употребу повезује са концептом надзорног капитализма, у којем подаци о понашању корисника постају значајан ресурс за предвиђање и усмеравање будућих поступака. Управо због тога питање приватности у дигиталним медијима више се не односи само на заштиту појединачних личних података, већ и на транспарентност алгоритамске селекције, ограничење профилисања и могућност корисника да задржи контролу над начином на који се његови подаци користе.

Циљ рада је да анализира однос дигиталних медија и заштите приватности са становишта људских права и сигурности података. Посебни циљеви односе се на идентификовање главних механизма ризика, анализу улоге профилисања и персонализације, разматрање утицаја вештачке интелигенције на аутентичност медијског садржаја и систематизацију релевантног регулаторног оквира. Полази се од тезе да се одржива дигитална комуникација не може градити искључиво на максимизацији прикупљања података, већ на пропорционалној обради, транспарентности и стварној контроли корисника.

ДИГИТАЛНИ МЕДИЈИ КАО ИНФРАСТРУКТУРА ПРИКУПЉАЊА ПОДАТАКА

Основна карактеристика савремених дигиталних медија јесте да се велики део њиховог функционисања заснива на подацима. Платформе бележе кликове, претраге, време проведено на одређеном садржају, реакције, коментаре, дељења, листе праћења, техничке податке о уређају, приближну локацију и друге дигиталне трагове. Појединачни податак може изгледати безначајно, али се његова вредност повећава када се повеже са већим бројем других сигнала. Тада постаје могуће формирање профила интересовања и предвиђање вероватноће одређене реакције корисника.

Профилисање се у том смислу не односи само на очигледне категорије као што су пол, старост или место становања. Савремени системи могу статистички процењивати интересовања, потрошачке навике, политичку заинтересованост, склоност одређеним темама и многе друге обрасце. Овакви закључци не морају бити тачни да би произвели последице: довољно је да алгоритам корисника сврста у одређени сегмент и да се на основу тог сегмента промени садржај који ће му бити приказан. Због тога приватност не подразумева само заштиту од откривања тајних информација, већ и заштиту од непрозирног категорисања.

Европска комисија у тумачењу принципа GDPR-а посебно наглашава законитост, правичност и транспарентност, ограничење сврхе, минимизацију података, ограничење чувања, тачност, интегритет и поверљивост, као и одговорност руковођа. Принцип минимизације има посебан значај за дигиталне медије: организација треба да прикупља само оне податке који су неопходни за конкретно дефинисану сврху, а не све податке које је технички могуће прикупити (European Commission, 2026a).

Практичан проблем представља чињеница да се обрада често одвија кроз велики број актера. Медијски портал може користити аналитичке алате, огласне мреже, сервисе за персонализацију, системе за мерење публице, спољне видео-платформе и cloud инфраструктуру. Корисник зато тешко може да процени колико организација учествује у обради његових података. Одговорност за приватност захтева да медијска организација разуме сопствени технички екосистем и да не третира услуге трећих страна као област за коју не сноси никакву одговорност.

Алгоритамско профилисање, персонализација и јавно мњење

Системи препорука представљају један од најважнијих механизма савремених дигиталних медија. Њихов циљ је да из великог броја доступних информација изабере садржај за који постоји највећа вероватноћа да ће привући пажњу конкретног корисника. Са становишта употребљивости, ова функција је оправдана: без алгоритамске селекције корисник би био изложен огромној количини нерелевантних информација. Проблем настаје када критеријуми селекције нису транспарентни, када се прекомерно ослањају на праћење понашања или када је једини циљ максимизација ангажовања.

Персонализација мења класичне механизме обликовања јавног мњења. У дигиталном окружењу не постоји један дневни ред за целокупну публику. Два корисника исте платформе могу истовремено бити изложена потпуно различитим темама, јер алгоритам формира индивидуализовани информациони ток. Јавност се тако фрагментира на велики број паралелних информационих окружења. Pariser (2011) је овај проблем популаризовао кроз концепт „filter bubble”, односно информационог мехура у којем корисник све чешће сусреће садржаје који су усклађени са његовим претходним интересовањима. Иако персонализација сама по себи не мора нужно довести до поларизације, ризик се повећава када алгоритми фаворизују садржај који производи снажне емоционалне реакције, конфликт или дуго задржавање. Тада економија пажње може постати важнија од јавног интереса.

Проблем приватности и проблем јавног мњења овде се непосредно додирују. Што систем има више података о кориснику, то прецизније може проценити која тема, формулација, визуелни елемент или емоционални оквир има највећу вероватноћу да изазове реакцију. У комерцијалном оглашавању то може значити релевантнију понуду. У политичкој комуникацији исти механизам може омогућити микротаргетирање различитих група порукама које широј јавности нису подједнако видљиве. Tufekci (2015) упозорава да алгоритамска агенција може производити друштвене последице које превазилазе појединачну интеракцију корисника са платформом.

Посебно осетљиво питање представља таргетирање на основу посебних категорија података или закључака који практично откривају осетљиве карактеристике. Европски одбор за заштиту података у Смерницама 8/2020 анализира правне основе и ризике таргетирања корисника друштвених мрежа, укључујући профилисање и online праћење (EDPB, 2020). DSA додатно забрањује таргетирање огласа на основу осетљивих података и профилисање оглашавања малолетницима када платформа са разумном сигурношћу зна да је корисник малолетан (European Commission, 2026b).

ПРИВАТНОСТ, БЕЗБЕДНОСТ ПОДАТАКА И ПРАВО НА КОНТРОЛУ

Заштита приватности не може се свести на формално приказивање политике приватности или банера за колачиће. Квалитет заштите зависи од тога да ли корисник може разумети ко обрађује његове податке, у коју сврху, на ком правном основу, колико дуго и са ким се подаци деле. GDPR и Закон о заштити података о личности Републике Србије постављају принципе који захтевају закониту, правичну и транспарентну обраду. Закон о заштити података о личности („Службени гласник РС”, бр. 87/2018) уређује права физичких лица, обавезе руковалаца и обрађивача и посебне случајеве обраде, а његова примена започела је 2019. године.

Контрола корисника мора бити стварна, а не само формална. Ако је прихватање праћења доступно једним кликом, док је одбијање сакривено иза више менија и нејасних формулација, кориснички избор је манипулативно обликован. DSA забрањује тзв. dark patterns, односно обмањујуће дизајнерске праксе које корисника наводе на одлуку коју иначе можда не би донео. Ово правило показује да се приватност не штити само текстом обавештења већ и архитектуром интерфејса.

Безбедност података је други неопходан елемент. Чак и када је прикупљање података законито, неодговарајуће мере заштите могу довести до неовлашћеног приступа, крађе идентитета, објављивања приватних информација или даље злоупотребе. Принцип интегритета и поверљивости зато захтева одговарајуће техничке и организационе мере, као што су контроле приступа, шифровање, псеудонимизација, ограничење привилегија и редовно ажурирање система. Приватност по дизајну подразумева да се ове мере планирају од почетка развоја услуге, а не тек након инцидента.

Посебан значај има процена утицаја на заштиту података код обрада које могу представљати висок ризик по права и слободе лица. У медијском и платформском окружењу то може бити релевантно за обимно профилисање, систематско праћење или обраду осетљивих података. Процена ризика не треба да буде схваћена као једнократна административна обавеза. Системи се мењају, додају се нови извори података и нови алгоритми, па је потребно периодично преиспитивање оправданости и пропорционалности обраде.

Конвенција 108 Савета Европе и њена модернизована верзија 108+ имају додатни значај јер заштиту података повезују са људским достојанством и информационом самоодређеношћу. Савет Европе наглашава да је интернет олакшао приступ и размену података, али истовремено створио нове прекограничне изазове за приватност. Модернизација Конвенције усмерена је на изазове нових информационо-комуникационих технологија и јачање ефективне примене стандарда (Council of Europe 2018, 2026).

Вештачка интелигенција, deepfake садржаји и нови ризици

Развој генеративне вештачке интелигенције додатно мења однос медија, приватности и информационе безбедности. Текст, фотографија, аудио и видео могу се генерисати или модификовати на начин који је све теже разликовати од аутентичног садржаја. Ова технологија има значајне креативне и продуктивне могућности, али истовремено снижава трошак производње убедљивих дезинформација, лажног представљања и deepfake материјала. Ризик за приватност може настати када се нечији лик, глас или други лични атрибути користе без знања и одобрења. Deepfake снимак може угрозити углед, безбедност, професионални статус и психолошки интегритет појединца, а последице су посебно тешке када се садржај вирусно прошири пре него што буде оповргнут. Поред тога, системи генеративне AI могу бити повезани са великим скуповима података чије порекло и законитост обраде кориснику нису очигледни. Регулаторни приступ Европске уније додатно је проширен Актом о вештачкој интелигенцији, који уводи посебне захтеве у погледу ризика и транспарентности одређених AI система (**European Parliament & Council of the European Union, 2024**).

AI Act Европске уније уводи транспарентност као један од механизма за смањење ових ризика. Европска комисија је у јулу 2026. објавила смернице за примену обавеза из члана 50 AI Act-а, које се примењују од 2. августа 2026. Одређени интерактивни AI системи морају кориснику јасно ставити до знања да комуницира са вештачком интелигенцијом, док AI-генерисани или манипулисани садржаји подлежу одређеним обавезама означавања и машински читљивог обележавања (European Commission, 2026c).

За медије је посебно важно правило које се односи на deepfake садржај и текстове о питањима од јавног интереса када су генерисани или манипулисани вештачком интелигенцијом без људске редакционе контроле. Сврха није забрана AI садржаја, већ смањење ризика од обмане и манипулације. Транспарентност постаје предуслов за очување поверења: публика мора имати довољно информација да процени природу и порекло садржаја.

Ипак, означавање само по себи није довољно. Одговорна употреба AI у медијима захтева уредничке процедуре за проверу чињеница, евиденцију начина на који је AI коришћен, заштиту поверљивих информација и ограничење уноса личних података у спољне AI системе. Посебно је важно да запослени разумеју да уношење интерних докумената, података о изворима или личних информација у јавне генеративне системе може створити нови канал ризика који класичне медијске процедуре раније нису обухватале.

Регулаторни оквир и одговорност дигиталних платформи

Регулаторни оквир дигиталног простора у Европи све више се развија као систем међусобно повезаних правила. GDPR поставља општи оквир обраде личних података. Ови принципи представљају основу европског система заштите личних података и утврђени су Општом уредбом о заштити података (**European Parliament & Council of the European Union, 2016**). DSA уређује одговорност посредничких услуга и платформи. AI Act уређује ризике и обавезе повезане са вештачком интелигенцијом. Ови инструменти се не могу посматрати изоловано јер једна дигитална услуга истовремено може обрађивати личне податке, користити систем препорука и интегрисати AI функције. Додатна правила о транспарентности оглашавања, системима препорука, забрани манипулативних интерфејса и заштити малолетника утврђена су Актом о дигиталним услугама (**European Parliament & Council of the European Union, 2022**).

DSA је посебно значајан за медијско окружење због правила о оглашавању и системима препорука. Огласи морају бити јасно означени и корисник треба да добије информацију о томе ко стоји иза огласа и зашто га види. Веома велике онлајн платформе морају омогућити и опцију неперсонализованог feed-а. На тај начин корисник добија већи степен контроле над критеријумима који одређују видљивост садржаја (European Commission, 2026b).

За медије и оглашиваче важна је и забрана таргетирања на основу осетљивих категорија података, као и посебна заштита малолетника. Оваква правила показују помак од модела у којем је корисник готово искључиво сам одговоран за избор ка моделу у којем и дизајн платформе мора бити прилагођен заштити права. Посебно је важно што се од платформи захтева да процењују системске ризике, укључујући ризике по грађански дискурс и фундаментална права.

У Републици Србији централни нормативни оквир за личне податке представља Закон о заштити података о личности, а независни надзорни орган је Повереник за информације од јавног значаја и заштиту података о личности. За домаће медије и организације од посебног је значаја чињеница да закон обухвата аутоматизовану обраду података и прописује права лица, обавезе руковалаца и обрађивача, као и механизме надзора и правне заштите. Повереник такође указује на обавезу одређивања лица за заштиту података у ситуацијама систематског надзора великог броја лица или обраде посебних категорија података у великом обиму.

Медијска специфичност захтева пажљиву равнотежу. Заштита приватности не сме постати инструмент гушења слободе изражавања и јавног интереса, али се ни право јавности да буде информисана не може користити као опште оправдање за произвољно објављивање личних података. Одговорна процена мора узети у обзир природу информације, јавни интерес, статус лица, потенцијалну штету и минималан обим података који је неопходан за разумевање теме.

Етички изазови медија и дигиталног оглашавања

Етика дигиталних медија проширује класичне новинарске принципе на питања која раније нису била у средишту уредничког рада. Поред тачности, објективности и заштите извора, данас се постављају питања начина прикупљања података, алгоритамске дистрибуције садржаја, аутоматизованог одлучивања и комерцијалног профилисања публике. Ризици профилисања постали су посебно видљиви након случаја Cambridge Analytica, који је показао како масовно прикупљање и анализа података са друштвених мрежа могу бити употребљени за психографско профилисање и политичко микротаргетирање (Isaak & Hanna, 2018). Одговорност медија зато више није ограничена само на текст или снимак који је објављен, већ и на техничке системе преко којих се тај садржај дистрибуира и монетизује.

Посебно осетљив сегмент представља native advertising и персонализовано оглашавање. Када је граница између уредничког и плаћеног садржаја нејасна, корисник може донети одлуку без разумевања комерцијалног интереса који стоји иза поруке. Ако се томе дода профилисање на основу понашања, медијска порука постаје истовремено садржај и инструмент утицаја. Због тога је транспарентност спонзорства, начина таргетирања и коришћења података важна за очување поверења.

Етички ризик постоји и онда када су праксе формално законите, али прекомерне. Дугачки услови коришћења могу испунити формалну обавезу информисања, а да корисник реално не разуме последице. Слично томе, профилисање засновано на легитимном интересу може бити формално образложено, али и даље непропорционално ако производи дубоке и дуготрајне профиле. Етички стандард зато треба да буде виши од минималног правног стандарда и да укључује питање шта корисник разумно очекује у конкретном контексту.

Одговорност је посебно важна у комуникацији усмереној ка деци и младима. Малолетници често немају исти ниво критичке процене комерцијалних и алгоритамских механизма као одрасли. DSA зато уводи посебне мере заштите и забрањује профилисање оглашавање малолетницима. За медије је то сигнал да дизајн, избор података и комерцијални модели намењени млађој публици морају бити засновани на појачаној заштити приватности, а не на максималном извлачењу пажње.

МОДЕЛ ОДГОВОРНЕ ДИГИТАЛНЕ КОМУНИКАЦИЈЕ

На основу анализираних ризика може се предложити модел одговорне дигиталне комуникације који се заснива на шест међусобно повезаних принципа: јасној сврси, минимизацији података, транспарентности, корисничкој контроли, безбедности и одговорности. Модел је применљив на медијске организације, онлајн платформе, јавне институције и друге субјекте који комуницирају са публиком у дигиталном простору.

Табела 1. Модел одговорне дигиталне комуникације

Принцип	Кључно питање	Практична примена
Јасна сврха	Зашто се подаци обрађују?	Сврха се дефинише пре прикупљања и не проширује се произвољно.
Минимизација	Који је најмањи неопходан скуп података?	Не прикупљају се подаци који нису потребни за конкретну услугу.
Транспарентност	Да ли корисник разуме шта се дешава?	Кратка и слојевита обавештења, објашњење препорука и огласа.
Контрола корисника	Може ли корисник стварно да изабере?	Једноставно одбијање праћења, измена преференција и повлачење сагласности.
Безбедност	Како се спречава неовлашћени приступ?	Контрола приступа, шифровање, псеудонимизација и редовно тестирање.
Одговорност	Ко проверава ризике и резултате?	Евиденције, процена утицаја, интерне контроле, обука и ревизија добављача.

Извор: систематизација аутора на основу GDPR, DSA, AI Act и смерница EDPB-а.

Први принцип је јасна сврха. Организација пре прикупљања података мора да зна који конкретан проблем решава. Формулације попут „унапређења корисничког искуства” нису довољно прецизне ако се под њима подразумева широк спектар накнадних обрада. Друга компонента је минимизација. Систем треба пројектовати тако да комуникациони циљ постиже са најмањим неопходним бројем података. Ово истовремено смањује правни, етички и безбедносни ризик. Трећи принцип је транспарентност. Информације о обради

морају бити кратке, разумљиве и доступне у тренутку када су кориснику потребне. Поред формалне политике приватности, савремене платформе треба да објасне зашто корисник види одређени оглас или препоруку. Четврти принцип је корисничка контрола: одбијање непотребног праћења не сме бити намерно компликованије од прихватања, а корисник треба да може да промени избор без непотребних препрека. Пети принцип је безбедност. Сваки додатни податак повећава вредност потенцијалног инцидента, због чега су ограничење приступа, псеудонимизација, шифровање и редовно тестирање неопходни. Шести принцип је одговорност. Организација мора бити у стању да покаже не само да поседује документе, већ и да су процеси у пракси усклађени са правилима. То подразумева јасне улоге, обуку запослених, управљање добављачима, евиденцију инцидената и периодичну ревизију алгоритама и огласних система.

Практична примена претходног модела може се приказати кроз матрицу у којој се сваки технолошки механизам повезује са типичним ризиком по приватност и одговарајућом мером заштите. Вредност овакве систематизације је у томе што омогућава да се питање приватности укључи у свакодневне уредничке, маркетиншке и техничке одлуке.

Табела 2. Кључни ризици и мере заштите

Механизам	Ризик	Могућа последица	Мера заштите
Online праћење	Прекомерно прикупљање	Губитак контроле и повећан ризик инцидента	Минимизација, рокови чувања, privacy by design
Профилисање	Непрозирна категоризација	Дискриминација, нетачни закључци, манипулација	Објашњење, правни основ, могућност приговора
Системи препорука	Филтер-мехури и појачавање екстремног садржаја	Сужавање информационог избора	Транспарентност параметара и непрофилисана опција где је применљиво
Таргетирано оглашавање	Осетљиви подаци и микротаргетирање	Повреда приватности и асиметричан утицај	Забрана осетљивог таргетирања, посебна заштита малолетника
Dark patterns	Манипулативни интерфејс	Привидна сагласност и губитак избора	Симетрични избори и јасан дизајн
Генеративна AI	Deerfake, лажно представљање, нејасно порекло	Обмана, репутациона штета, дезинформације	Означавање, људска контрола, верификација садржаја

Извор: систематизација аутора

Практична примена заштите приватности у медијским организацијама треба да започне мапирањем токова података. Организација мора знати које податке прикупља директно од корисника, које податке генеришу аналитички алати, које податке добијају огласни партнери и где се подаци физички или логички чувају. Без такве мапе тешко је проценити ризик, одредити рокове чувања или проверити да ли се исти податак користи у сврхе које кориснику нису биле јасно представљене. За медије је посебно важно да техничка одељења, маркетинг и правна служба не делују одвојено, јер се већина ризика јавља управо на граници између уредничких, комерцијалних и техничких процеса.

Друга препорука односи се на огласне и аналитичке технологије. Сваки tracker, pixel или SDK треба да има јасно образложену функцију и власника процеса унутар организације. Потребно је периодично уклонити алате који се више не користе и ограничити пренос података трећим странама. Посебну пажњу треба посветити уговорима са добављачима, месту обраде, механизмима за пренос података и могућности да добављач користи податке за сопствене сврхе. Принцип минимизације треба применити и на мерење публике: није свака метрика која је доступна истовремено и неопходна за пословну одлуку.

Трећа препорука односи се на редакцијску употребу вештачке интелигенције. Медији треба да усвоје интерна правила која одређују у којим ситуацијама се AI може користити за транскрипцију, превођење, резимирање, генерисање наслова или визуелног материјала, као и када је обавезна људска провера. Посебно треба забранити уношење поверљивих извора, необјављених истраживачких материјала и осетљивих личних података у јавне AI системе без претходне процене ризика. Када AI значајно учествује у стварању садржаја од јавног интереса, транспарентно обавештавање публике треба посматрати као део професионалне одговорности, чак и у случајевима у којима закон не прописује детаљан облик обавештења.

Четврта препорука односи се на управљање инцидентима. Медијске куће су атрактивна мета јер поседују податке о претплатницима, запосленима, изворима, комерцијалним партнерима и интерним истраживањима. Потребно је успоставити процедуру која дефинише ко процењује инцидент, ко доноси одлуку о обавештавању надзорног органа и лица на која се подаци односе, ко комуницира са јавношћу и како се чувају докази о инциденту. Вежбе реаговања и јасни контакти могу значајно смањити време реакције и последице повреде података. На тај начин се приватност повезује са ширим концептом сајбер безбедности и отпорности медијске организације.

Увођење показатеља одговорности који нису искључиво финансијски представља пету препреку. Поред броја прегледа, времена задржавања и прихода од огласа, организација може пратити број активних trackers-a, време решавања захтева корисника, број инцидентата, проценат добављача који су прошли процену приватности и број запослених који су завршили обуку. Овакви показатељи омогућавају руководству да приватност посматра као мерљив елемент квалитета управљања. Они такође олакшавају доказивање одговорности и подстичу културу у којој се ризици препознају пре него што прерасту у правни или репутациони проблем.

Анализа показује да се приватност у дигиталним медијима не може успешно штитити једним инструментом. Правни оквир је неопходан, али не може унапред предвидети сваку нову техничку праксу. Техничке мере су неопходне, али саме по себи не решавају проблем непрозирног профилисања или манипулативног интерфејса. Медијска писменост је важна, али није оправдано целокупну одговорност пребацити на корисника. Потребан је интегрисани приступ у којем се право, технологија, организациона одговорност и етика међусобно допуњују.

Посебно је важно превазићи схватање да је приватност препрека иновацијама. Добро осмишљена заштита података може побољшати квалитет дигиталне услуге зато што организацију приморава да јасније дефинише сврху, уклони непотребне токове података и

кориснику понуди разумљивији однос. На тај начин приватност постаје елемент поверења, а поверење представља критичан ресурс за медије чији кредибилитет зависи од перцепције професионалности и одговорности.

ЗАКЉУЧАК

Дигитални медији су створили информационо окружење у којем се право на приватност, слобода изражавања и право јавности на информисање све чешће преплићу. Подаци о кориснику постали су централни ресурс за алгоритамску селекцију, персонализацију и оглашавање, због чега се медијска комуникација више не може анализирати одвојено од начина на који се подаци прикупљају и обрађују. Најзначајнији ризици односе се на прекомерно праћење, непрозирно профилисање, микротаргетирање, манипулативни дизајн интерфејса, неадекватну безбедност и све већу производњу AI-генерисаног или манипулисаног садржаја. Ови ризици могу угрозити не само приватност појединца већ и квалитет јавног дискурса, јер алгоритми утичу на видљивост тема и на услове под којима корисници формирају ставове. Одговор на наведене изазове мора бити вишеслојан. GDPR, DSA, AI Act, Конвенција 108+ и национални прописи обезбеђују важан нормативни оквир, али стварна заштита зависи од начина на који се правила преводе у дизајн система и свакодневне организационе праксе. Минимизација података, транспарентност, корисничка контрола, приватност по дизајну, адекватне безбедносне мере и континуирана процена ризика представљају кључне елементе одговорног модела. Уместо концепта у којем је најбоља дигитална услуга она која о кориснику зна највише, потребно је развијати приступ у којем се квалитет мери способношћу да се релевантна информација пружи уз најмањи неопходан обим података. Тако приватност постаје не само правна обавеза већ фактор квалитета, поверења и дугорочне одрживости дигиталних медија. Управо у томе лежи кључна равнотежа дигиталног доба: технологија треба да проширује људске могућности, а не да аутономију појединца претвара у ресурс којим се непрозирно управља.

РЕФЕРЕНЦЕ

Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+). Strasbourg: Council of Europe.

Council of Europe. (2026). Protection of personal data and privacy. Council of Europe Portal.

European Commission. (2026a). Principles of the GDPR. Brussels: European Commission.

European Commission. (2026b). Digital Services Act: Questions and answers. Shaping Europe's Digital Future.

European Commission. (2026c). Guidelines on transparency obligations for providers and deployers of AI systems under Article 50 of the AI Act. Brussels: European Commission.

European Data Protection Board. (2020). Guidelines 8/2020 on the targeting of social media users (Version 2.0). Brussels: EDPB. https://www.edpb.europa.eu/public-consultations/guidelines-082020-on-the-targeting-of-social-media-users_en

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1-88.

European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). *Official Journal of the European Union*, L 277, 1-102.

European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.

Gillespie, T. (2014). The relevance of algorithms. *Media technologies: Essays on communication, materiality, and society*, 167(2014), 167.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, 51(8), 56–59. <https://doi.org/10.1109/MC.2018.3191268>

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. penguin UK.

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Tech. LJ*, 13, 203.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. <https://doi.org/10.1057/jit.2015.5>

Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs. *Revista Española de Educación Comparada*. ISSN, 2174-5382.

Закон о заштити података о личности. (2018). Службени гласник Републике Србије, бр. 87/2018.

УПОТРЕБА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У НОВИНСКИМ РЕДАКЦИЈАМА И РИЗИЦИ ПО ПРИВАТНОСТ ГРАЂАНА

Милена Шовић¹

Сажетак

Развој и све шира примена вештачке интелигенције (ВИ) значајно мењају начин рада савремених новинских редакција, омогућавајући аутоматизацију појединих фаза производње, обраде и дистрибуције медијског садржаја. Истовремено, употреба ВИ технологија отвара значајна питања у погледу заштите права на приватност и безбедности личних података грађана, новинарских извора и других лица чији се подаци обрађују у процесу новинарског рада. Циљ рада је да се анализирају начини примене вештачке интелигенције у новинским редакцијама, са посебним освртом на ризике које таква примена може представљати за приватност грађана и поверљивост новинарских извора. Посебна пажња посвећена је обради личних података у ВИ системима, могућности цурења и неовлашћене употребе података, ризику од деанонимизације извора, као и профилисању и аутоматизованој анализи понашања корисника. У раду се разматра и постојећи правни и етички оквир, укључујући националне прописе о заштити података о личности, Општу уредбу о заштити података Европске уније (GDPR), релевантне међународне стандарде и професионалне етичке принципе новинарства. Анализа указује на потребу за успостављањем јасних интерних правила за употребу ВИ алата у редакцијама, применом принципа минимизације података, проценом ризика пре обраде осетљивих информација и очувањем професионалне одговорности новинара. Одговорна примена вештачке интелигенције подразумева успостављање равнотеже између технолошких могућности, права грађана на приватност и основних принципа новинарске професије.

Кључне речи: вештачка интелигенција, новинарство, новинске редакције, приватност, лични подаци, новинарски извори, заштита података, медијска етика.

¹ Факултет за економију и инжењерски менаџмент, „ФИМЕК” Нови Сад, Србија
e-mail: milena.sovich@gmail.com

УВОД

Развој и све шира примена вештачке интелигенције последњих година значајно су променили начин на који се новинарски садржај прикупља, обрађује, производи и дистрибуира. Вештачка интелигенција више није ограничена на експерименталну употребу, већ постаје део свакодневне праксе новинских редакција. Њена примена обухвата транскрипцију, превођење, анализу великих скупова података, генерисање и прилагођавање садржаја, као и персонализацију и препоручивање вести. Према истраживању Reuters Institute-a, медијске организације све интензивније уводе генеративну вештачку интелигенцију у различите сегменте редакцијског рада, посебно у аутоматизацију процеса, персонализацију, креирање садржаја и прикупљање и анализу информација (Newman & Cherubini, 2025).

Поред технолошких и организационих предности, примена вештачке интелигенције отвара и питања која се односе на заштиту приватности и личних података. У новинарском раду могу се обрађивати подаци о лицима која су предмет извештавања, новинарским изворима, сведоцима, жртвама и другим учесницима у процесу прикупљања и обраде информација. Употреба ВИ система у таквим процесима може повећати ризик од неовлашћеног приступа, откривања или даље употребе података, нарочито када се поверљиви материјали обрађују посредством екстерних система над којима редакција нема потпуну контролу (Cools & Diakopoulos, 2024; Jones & Galanos, 2024).

Новинарство има важну улогу у информисању јавности и откривању информација од јавног интереса, али та улога не искључује обавезу одговорног поступања са подацима о личности и заштите поверљивих извора. Истовремено, употреба ВИ у персонализацији и препоручивању садржаја отвара додатна питања у вези са обимом обраде података, транспарентношћу алгоритамских процеса и контролом корисника над употребом њихових података (Ross Arguedas, 2025). Због тога се примена ВИ у новинарству не може посматрати искључиво као питање технолошке ефикасности, већ и као питање професионалне, правне и етичке одговорности.

Проблем заштите приватности додатно добија на значају у контексту развоја генеративне вештачке интелигенције, јер новинарски рад све више укључује алате способне да обрађују велике количине текста, докумената и других информација. Истовремено, истраживања показују да публика има различит степен прихватања ВИ у зависности од њене улоге у производњи вести, при чему се веће поверење задржава када ВИ има помоћну, а не водећу улогу у новинарском процесу (Simon et al., 2025), што указује на потребу да се технолошки развој прати одговарајућим механизмима транспарентности, људског надзора и професионалне одговорности.

Имајући у виду наведене изазове, употребу вештачке интелигенције у новинским редакцијама неопходно је посматрати кроз истовремено технолошку, правну и етичку перспективу. Одговорна примена ВИ подразумева не само коришћење њених потенцијала за унапређење новинарског рада, већ и процену могућих последица по права грађана и безбедност новинарских извора. Управо потреба за успостављањем равнотеже између технолошких могућности, права на приватност и слободе информисања представља полазиште овог рада. **У складу са наведеним, циљ рада је да се анализирају начини примене вештачке интелигенције у новинским редакцијама, са посебним освртом на ризике које таква примена може представљати за приватност грађана и поверљивост новинарских извора.**

МЕТОДОЛОГИЈА РАДА

Рад је конципиран као научни прегледни рад, заснован на анализи и синтези релевантне научне и стручне литературе из области вештачке интелигенције, новинарства, медија, заштите приватности и података о личности. Основни циљ прегледа литературе био је да се сагледају начини примене вештачке интелигенције у новинским редакцијама и идентификују кључни ризици које њена употреба може представљати за приватност грађана и поверљивост новинарских извора.

Литература је одабрана према њеној релевантности за предмет и циљ рада, при чему су предност имали научни радови објављени у релевантним научним часописима, извештаји признатих истраживачких и академских институција, као и званични документи међународних и националних институција. Преглед је обухватио литературу објављену у периоду од 2021. до 2025. године, уз посебан фокус на новије изворе из 2024. и 2025. године, како би се обухватили најзначајнији савремени трендови у примени генеративне вештачке интелигенције у новинарству. Поред научне и стручне литературе, анализирани су и релевантни правни и етички документи који уређују питања заштите података о личности, приватности, слободе изражавања и употребе вештачке интелигенције у медијима.

Приликом избора литературе примењени су следећи критеријуми: директна тематска повезаност са предметом рада, релевантност за постављени циљ, актуелност извора и поузданост аутора или институције која је извор објавила. Посебно су разматрани извори који се односе на примену вештачке интелигенције у новинарским редакцијама, аутоматизацију и генерисање садржаја, анализу података, персонализацију и системе препоруке, као и на ризике повезане са обрадом личних података, профилисањем, цурењем података и заштитом новинарских извора.

Анализирана литература систематизована је према основним тематским целинама рада. Најпре су издвојени начини примене вештачке интелигенције у новинарству, а затим су анализирани ризици по приватност који могу настати током прикупљања, обраде, чувања и коришћења података. Посебна пажња посвећена је обради личних и поверљивих података у ВИ системима, могућности неовлашћеног приступа и цурења података, ризику од деанонимизације новинарских извора, као и профилисању и персонализацији медијских садржаја.

Поред анализе научне и стручне литературе, спроведена је и анализа релевантног правног и етичког оквира. У том делу разматрани су Закон о заштити података о личности Републике Србије, Општа уредба о заштити података о личности Европске уније (GDPR), Европски акт о слободи медија, релевантни међународни стандарди, смернице Савета Европе, Препорука UNESCO-а о етици вештачке интелигенције и Кодекс новинара и новинарки Србије. Ови извори коришћени су ради сагледавања односа између употребе ВИ технологија, права на приватност, заштите података о личности, слободе изражавања и професионалне одговорности медија. У анализи је примењен критички и компаративни приступ, којим су упоређиване користи и потенцијални ризици примене ВИ у новинарству.

ПРИМЕНА ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У НОВИНСКИМ РЕДАКЦИЈАМА

Примена вештачке интелигенције у новинским редакцијама више се не своди на експерименталну употребу појединачних алата, већ постепено постаје део различитих фаза новинарског процеса. Развој машинског учења, обраде природног језика и генеративне вештачке интелигенције омогућио је аутоматизацију појединих рутинских задатака, бржу обраду информација и прилагођавање садржаја различитим потребама публике. Истраживања показују да медијске организације ВИ све више користе не само за производњу садржаја већ и за истраживање, анализу података, превођење, персонализацију и препоручивање вести (Lopezosa et al., 2024; Newman & Cherubini, 2025).

Једна од највидљивијих примена генеративне вештачке интелигенције у новинарству односи се на генерисање, уређивање и прилагођавање медијског садржаја. Савремени језички модели могу да помогну новинарима у креирању наслова, сажетака, почетних верзија текстова, предлога за структуру чланка и прилагођавању већ написаног садржаја различитим форматима и циљним групама. Истраживање спроведено међу новинарима у Уједињеном Краљевству показало је да се ВИ, поред транскрипције и превођења, користи за истраживање тема, генерисање идеја, израду делова текстова, укључујући наслове, као и за израду првих верзија новинарских текстова (Thurman et al., 2025).

Генеративна ВИ може посебно бити корисна у ситуацијама у којима је потребно брзо обрадити велики број информација или исти садржај прилагодити различитим комуникационим форматима. Reuters Institute наводи да медијске организације већ развијају интерне ВИ алате који обухватају функције као што су предлагање наслова, сажимање текста, исправљање језичких грешака и израда нацрта на основу основних чињеница (Newman & Cherubini, 2025).

Међутим, примена генеративних система у производњи садржаја не подразумева аутоматско преношење уређивачке одговорности на алгоритам. Један од основних проблема односи се на могућност појаве нетачних или контекстуално непотпуних информација, као и на питање транспарентности у погледу начина на који је садржај произведен. Истраживања о ставовима новинара показују да се генеративна ВИ истовремено доживљава као средство за повећање ефикасности и као технологија која носи ризике у погледу тачности, ауторства, професионалне одговорности и поверења публике (Cools & Diakopoulos, 2024).

Због тога се у савременој новинарској пракси све више развија модел у којем ВИ делује као подршка новинару, а не као потпуна замена за његов професионални суд. Овај приступ је у складу и са налазима о ставовима публике: истраживање Reuters Institute-а показује да су корисници знатно прихватљивији према примени ВИ када човек задржава водећу или надзорну улогу у процесу производње вести, док је прихватање потпуно аутоматизованог новинарског садржаја знатно ниже (Simon et al., 2025).

Превођење представља једну од практично најзаступљенијих примена вештачке интелигенције у новинарском раду. Системи за обраду природног језика омогућавају брзо превођење текстова са једног језика на други, чиме се смањује време потребно за припрему вести за различита језичка тржишта. Поред самог превођења, ВИ може да помогне и у прилагођавању садржаја језичком, културном и контекстуалном окружењу одређене публике.

Подаци о професионалној употреби ВИ међу новинарима потврђују значај ове функције. У истраживању Reuters Institute-а, 33% британских новинара навело је да ВИ користи

за превођење најмање једном месечно, што ову примену сврстава међу најчешће облике професионалне употребе ВИ, одмах уз транскрипцију и титловање и проверу граматике и уређивање текста (Thurman et al., 2025).

Превођење посредством ВИ система има значај и са становишта доступности информација. Reuters Institute у извештају о употреби генеративне ВИ у вестима наводи да публика показује релативно висок ниво прихватања употребе ВИ за превођење новинских текстова, при чему је 24% испитаника исказало интересовање за ову могућност као облик персонализације вести (Simon et al., 2025).

Ипак, аутоматско превођење у новинарству захтева људску контролу, нарочито код текста који садржи специфичну терминологију, правне и политичке појмове, изјаве извора или културно осетљиве информације. Грешка у преводу новинарског текста може изменити значење изворне информације и тиме непосредно утицати на тачност извештавања. Због тога употреба ВИ за превођење треба да буде схваћена као помоћни процес који захтева редакцијску проверу, а не као потпуно аутономна замена за професионалног преводиоца или новинара.

Једна од значајних предности вештачке интелигенције у новинарству односи се на могућност брзе обраде великих и структурно сложених скупова података. Новинари који се баве истраживачким и податковним новинарством могу користити ВИ системе за проналажење образаца, класификацију докумената, издвајање релевантних информација, транскрипцију аудио и видео материјала, претраживање великих архива и повезивање информација из различитих извора.

Систематски преглед истраживања о трансформацији дигиталних редакција показује да је анализа података једна од значајнијих области примене ВИ у новинарству. Аутори посебно указују на способност ВИ система да обрађују велике количине информација и подрже новинаре у задацима који би ручном анализом захтевали значајно више времена (Sonni et al., 2024).

Значај ВИ за истраживачко новинарство посебно долази до изражаја код обраде великих документарних база. Reuters Institute наводи примере редакција које ВИ користе за истраживање тема, податковно новинарство и истраге, при чему се технологија примењује на распршене изворе и велике количине материјала како би се брже идентификовале релевантне информације и потенцијалне везе између података (Newman & Cherubini, 2025).

Међутим, управо ова област отвара једно од најзначајнијих питања за тему овог рада. Документарни материјали који се анализирају у истраживачком новинарству могу садржати личне податке, податке о жртвама, сведоцима, изворима и другим лицима. Уношење таквих материјала у ВИ систем може створити додатни ризик уколико редакција нема јасну контролу над начином на који се подаци чувају, обрађују или евентуално даље користе. Због тога повећана аналитичка способност ВИ система истовремено захтева строжи приступ управљању подацима и заштити поверљивих информација.

Персонализација представља још једну важну област примене вештачке интелигенције у савременим медијима. Системи персонализације и препоруке анализирају различите облике интеракције корисника са медијским садржајем, укључујући претходно читане текстове, интересовања и друге показатеље понашања, како би кориснику понудили садржај који је процењен као релевантан. ВИ тако може утицати не само на производњу вести већ и на њихову дистрибуцију и начин на који појединачни корисници долазе до информација.

Reuters Institute је у истраживању за 2025. годину утврдио да 80% медијских издавача сматра да ће употреба ВИ за побољшање персонализације и препоруке садржаја бити значајна у наредном периоду. Истовремено, медијске организације истражују могућности коришћења генеративне ВИ за сажимање текстова, прилагођавање њиховог формата и превођење, односно за обликовање вести према специфичним потребама појединачних корисника (Newman & Cherubini, 2025).

Сличан тренд уочава се и у ставовима публике. Према Digital News Report 2025, 27% испитаника заинтересовано је за сажете верзије новинских текстова, 24% за њихово превођење, а 21% за боље препоруке вести. Истовремено, публика показује већу резерву према персонализацији која непосредно одређује које ће вести корисник видети, што се може повезати са страхом од пропуштања важних информација и ограничења тематске разноврсности (Newman & Cherubini, 2025).

Персонализација зато има двоструки карактер. Са једне стране, она може повећати релевантност садржаја и олакшати кориснику приступ великом броју информација. Са друге стране, захтева прикупљање и анализу података о понашању корисника, чиме се отварају питања приватности, профилисања и транспарентности алгоритаМСКОГ одлучивања. Уколико корисник нема јасну информацију о томе који се подаци прикупљају, у које сврхе се користе и на који начин утичу на избор садржаја који му се приказује, персонализација може прерасти из механизма за побољшање корисничког искуства у инструмент интензивног праћења и профилисања.

Примена ВИ у новинским редакцијама показује као процес који истовремено повећава оперативну ефикасност медија и отвара нове професионалне, етичке и правне изазове. Од генерисања текста и превођења, преко анализе великих скупова података, до персонализације и препоруке садржаја, ВИ постепено продире у различите фазе новинарског рада. Управо ширина тих примена чини питање заштите приватности посебно значајним, јер се подаци о грађанима могу појавити у различитим фазама процеса – од прикупљања информација и истраживања до њихове обраде, чувања и дистрибуције.

РИЗИЦИ ПО ПРИВАТНОСТ ГРАЂАНА И ИЗВОРА

Примена вештачке интелигенције у новинским редакцијама, поред значајних предности у погледу брзине обраде информација, аутоматизације појединих поступака и могућности анализе великих количина података, отвара и низ питања која се односе на заштиту приватности и личних података. Посебан проблем представља чињеница да се ВИ системи у новинарству могу користити над материјалима који садрже податке о грађанима, сведоцима, жртвама, јавним личностима, али и над информацијама које омогућавају идентификацију поверљивих новинарских извора. У том контексту, ризик по приватност не настаје само приликом објављивања медијског садржаја, већ и у ранијим фазама прикупљања, обраде, анализе и чувања информација унутар редакције (Jones & Galanos, 2024).

Посебну сложеност овом проблему даје чињеница да ВИ системи могу повезивати и анализирати велики број различитих информација, укључујући податке који појединачно можда не откривају идентитет одређеног лица, али њиховом комбинацијом могу омогућити његову идентификацију. Због тога се питање заштите приватности у новинарском раду са ВИ технологијама не може свести само на забрану директног откривања имена, адресе или других очигледних идентификатора, већ обухвата и начин прикупљања, повезивања, обраде и даљег коришћења података. Савет Европе посебно наглашава значај заштите приватности и података, људског надзора и одговорности приликом увођења ВИ система у новинарску производњу (Council of Europe, 2024г).

Један од основних ризика повезаних са применом вештачке интелигенције у новинарству односи се на обраду личних података. Новинари током истраживања прикупљају различите

врсте информација које могу садржати идентификационе, контактне, финансијске, здравствене, професионалне и друге податке о личности. У традиционалном новинарском процесу такви подаци могу бити садржани у документима, електронској пошти, интервјуима, транскриптима, фотографијама, судским списима или интерним белешкама. Увођењем ВИ алата у процес обраде отвара се могућност да се део таквог материјала пренесе у информациони систем који није под директном контролом саме редакције.

Овај ризик је нарочито изражен код генеративних ВИ система који омогућавају аутоматску анализу докумената, сумирање интервјуа, издвајање информација из већег броја докумената или генерисање текста на основу достављеног материјала. Уколико новинар у такав систем унесе оригиналне документе који садрже податке о личности, поверљиве изворе или осетљиве информације, питање заштите података више није ограничено на унутрашњу инфраструктуру редакције. Подаци могу постати део обраде коју спроводи спољни технолошки провајдер, што захтева пажљиву процену услова коришћења конкретних ВИ алата, начина чувања података и мера информационе безбедности.

Управо због тога Савет Европе у смерницама за одговорну примену ВИ у новинарству наглашава потребу да медијске организације приликом избора и увођења ВИ система процене њихове последице по људска права, укључујући приватност и заштиту података. Одговорна примена ВИ не подразумева само проверу квалитета генерисаног текста већ и контролу начина на који се подаци прикупљају, обрађују и чувају (Council of Europe, 2024г).

Посебан проблем представљају осетљиви подаци који се могу појавити у истраживачком новинарству. На пример, новинарска документација може садржати податке о здравственом стању лица, жртвама кривичних дела, малолетним лицима, сведоцима, политичким или професионалним везама, финансијским трансакцијама или другим околностима из приватног живота. Њихово уношење у ВИ систем без претходне процене ризика може довести до нарушавања поверљивости и створити додатне ризике за лица на која се подаци односе.

Због тога принцип минимизације података има посебан значај у примени ВИ у новинарству. Уместо аутоматског преношења целокупног документа или базе података у ВИ систем, редакције би требало да процене који је минимални обим информација неопходан за конкретан задатак. Овакав приступ истовремено смањује ризик од неовлашћеног откривања података и омогућава ефикаснију контролу над информацијама које се обрађују.

Поред саме обраде личних података, значајан ризик представља могућност њиховог цурења, неовлашћеног приступа или употребе у сврхе које нису биле предвиђене у тренутку њиховог прикупљања. Ризик постоји како услед техничких пропуста и безбедносних рањивости, тако и услед неодговарајућег поступања запослених у редакцији. У пракси, један од проблема може настати онда када новинар, у намери да убрза рад, користи јавно доступан ВИ алат за обраду материјала који садржи поверљиве или личне податке.

Посебно је проблематично што корисник не мора увек имати потпуни увид у начин на који конкретна ВИ платформа обрађује достављене информације. Подаци могу бити обрађивани у сложеној инфраструктури која укључује различите сервере, добављаче услуга и системе за складиштење и обраду. Из перспективе редакције, то значи да употреба ВИ алата представља и питање управљања подацима, а не само питање технолошке ефикасности.

Истраживања о примени генеративне ВИ у новинарству указују да новинари препознају бројне ризике повезане са употребом ових технологија, при чему се питања тачности, контроле, одговорности и професионалне праксе преплићу са питањима безбедности и поверења (Cools & Diakoroulos, 2024). У том смислу, проблем није ограничен само на могућност да ВИ генерише нетачан садржај. Једнако значајно питање јесте шта се дешава са подацима који су коришћени за добијање таквог резултата.

Последице евентуалног цурења података у новинарском контексту могу бити озбиљније него у неким другим областима. Објављивање или неовлашћено откривање података може довести до нарушавања приватности, угрожавања безбедности појединаца, репутационе штете, откривања поверљивих односа или угрожавања новинарског извора. У случају осетљивих истраживачких прича, последице могу обухватити и физичку или професионалну угроженост лица која су новинарима доставила информације.

Посебно осетљиво питање представља заштита поверљивих новинарских извора. Поверљивост извора представља један од основних услова за обављање истраживачког новинарства, јер лица која достављају информације од јавног интереса често то чине под условом да њихов идентитет неће бити откривен. Увођење ВИ система у обраду новинарског материјала може, међутим, створити нове начине за повезивање информација и посредно откривање идентитета извора.

Деанонимизација се може догодити када ВИ систем комбинује више наизглед неповезаних информација. На пример, комбинација радног места, временског периода, места догађаја, функције коју лице обавља и специфичности информације коју је извор доставио може бити довољна да се идентификује конкретна особа. У том случају идентитет извора није откривен непосредним навођењем његовог имена, већ повезивањем више индиректних идентификатора.

Ризик је посебно значајан код истраживачког новинарства, где се често анализирају велике количине докумената. ВИ системи могу бити веома корисни у класификацији, претраживању и повезивању информација, али управо та способност повећава могућност да се из скупа података изведу закључци који нису били очигледни приликом појединачне анализе докумената. Због тога анонимизација мора бити схваћена као процес смањења могућности идентификације, а не само као механичко уклањање имена и презимена.

Смернице Савета Европе наглашавају значај заштите права и интереса лица која су предмет новинарског извештавања, као и потребу за одговарајућим људским надзором над употребом ВИ система. У новинарском контексту то подразумева да одлука о томе да ли се одређени документ или информација сме унети у ВИ систем не може бити препуштена само техничким могућностима алата (Council of Europe, 2024г).

Проблем заштите извора истовремено показује да приватност у новинарству има шири значај од заштите индивидуалног интереса једног лица. Уколико потенцијални извори стекну утисак да употреба дигиталних и ВИ система може довести до њихове идентификације, они могу бити мање спремни да сарађују са новинарима. На тај начин технолошки ризик може посредно утицати и на слободу медија, квалитет истраживачког новинарства и право јавности да буде информисана.

Још једна значајна област ризика односи се на профилисање грађана путем ВИ система. Профилисање подразумева аутоматизовану анализу података ради процене или предвиђања одређених карактеристика, интересовања, понашања или преференција појединца. У медијском окружењу такви системи могу бити повезани са персонализацијом садржаја, препорукама вести, анализом понашања публике и предвиђањем интересовања корисника.

Иако персонализација може побољшати корисничко искуство и повећати релевантност садржаја, она истовремено отвара питање граница до којих медијске организације треба да анализирају понашање своје публике. Што је већи број података који се прикупља о кориснику, већа је могућност стварања детаљног профила његових интересовања, навика и понашања. У комбинацији са ВИ системима, таква обрада може постати сложенија и мање транспарентна за самог корисника.

Савет Европе у својим смерницама за примену ВИ у новинарству препознаје персонализацију као област у којој је неопходно обезбедити транспарентност, заштиту приватности и одговарајући

степен људског надзора. Посебно је важно да корисници буду информисани о значајним аспектима аутоматизованог одлучивања и да имају могућност да разумеју начин на који се персонализовани садржај формира (Council of Europe, 2024г).

Профилисање може имати последице и по начин на који грађани долазе до информација. Ако алгоритам на основу претходног понашања корисника непрекидно препоручује сличне садржаје, може доћи до сужавања информационог окружења појединца. Иако ова појава није искључиво питање приватности, она је са њом повезана јер се персонализација заснива на континуираној обради података о понашању корисника. На тај начин граница између технолошке оптимизације медијског садржаја и интензивног праћења корисника постаје све мање јасна.

Питање профилисања у новинарству зато мора бити разматрано у ширем контексту односа између права на приватност и слободе информисања. У Србији је овај однос посебно значајан јер национални оквир заштите података о личности мора бити усклађен са потребом да се обезбеди слобода изражавања и информисања. Савет Европе истиче да члан 85 GDPR-а управо успоставља потребу за равнотежом између заштите личних података и слободе изражавања и информисања, што је од посебног значаја за новинарски рад (European Parliament & Council of the European Union, 2016).

Ризици по приватност у примени вештачке интелигенције у новинарству, дакле, не произлазе само из могућности техничког цурења података. Они обухватају читав процес – од прикупљања и уноса информација у ВИ систем, преко њихове обраде и повезивања, до чувања, профилисања и евентуалног даљег коришћења. Посебно место у овом процесу има заштита поверљивих извора, јер њихова идентификација може угрозити не само приватност појединца већ и његову безбедност и спремност других лица да сарађују са медијима. Због тога одговорна употреба ВИ у новинским редакцијама захтева процену ризика пре обраде података, минимизацију обима података, употребу безбедних система, јасне интерне протоколе и обавезан људски надзор над поступцима који могу имати последице по права појединаца.

ПРАВНИ И ЕТИЧКИ ОКВИР УПОТРЕБЕ ВИ У НОВИНАРСТВУ

Употреба вештачке интелигенције у новинарству одвија се на пресеку више правних и етичких области, јер истовремено обухвата питања заштите података о личности, приватности, слободе изражавања и информисања, заштите новинарских извора, професионалне одговорности и транспарентности медијског рада. Посебан изазов представља чињеница да се развој ВИ технологија одвија брже од измена традиционалних правних и професионалних норми. Због тога се одговорна употреба ВИ у новинарству не може заснивати само на постојећим законским одредбама, већ захтева њихово повезивање са новим смерницама, етичким кодексима и интерним правилима медијских организација.

У Републици Србији основни нормативни оквир за заштиту личних података представља **Закон о заштити података о личности** („Службени гласник РС”, бр. 87/2018). Закон уређује права физичких лица у вези са обрадом њихових података о личности, обавезе руковалаца и обрађивача, као и услове под којима је обрада података дозвољена. За примену вештачке интелигенције у новинарству посебно су значајна правила која се односе на законитост, ограничење сврхе, сразмерност и заштиту података током њихове обраде.

Посебан значај има члан 88. Закона о заштити података о личности, којим се уређује однос заштите података о личности и слободе изражавања и информисања. Овом одредбом предвиђена је могућност ограничења примене **конкретно наведених одредаба Закона** на обраду података о личности која се врши у сврхе новинарског истраживања и објављивања информација у медијима, али само уколико је такво ограничење у конкретном случају неопходно ради заштите слободе изражавања и информисања. Дакле, члан 88 не представља опште изузеће новинарства од примене прописа о заштити података о личности, већ успоставља механизам за усклађивање права на заштиту података са слободом изражавања и информисања, уз процену неопходности ограничења у конкретном случају. Законодавац тако настоји да успостави равнотежу између заштите приватности и слободе медија, имајући у виду значај новинарства за остваривање јавног интереса (Закон о заштити података о личности, 2018).

Наведени принцип је од посебног значаја у контексту ВИ технологија. Новинарско истраживање може захтевати обраду великих количина личних података, укључујући податке садржане у судским документима, базама података, интервјуима и другим материјалима од јавног интереса. Међутим, чињеница да се подаци обрађују у новинарске сврхе не значи да су сви облици њихове обраде аутоматски дозвољени. Приликом употребе ВИ система и даље је неопходно водити рачуна о оправданости, сразмерности и начину обраде података.

Значајан референтни оквир представља и **Општа уредба Европске уније о заштити података (GDPR)**. Иако GDPR није општи национални пропис Републике Србије, његов значај за медије и дигиталне платформе је велики, нарочито у ситуацијама у којима се обрађују подаци лица у Европској унији или када медијске организације послују у оквиру европског дигиталног простора. GDPR поставља основне принципе обраде података, међу којима су законитост, правичност и транспарентност, ограничење сврхе, минимизација података, тачност, ограничење чувања, интегритет и поверљивост, као и одговорност руковођаца ((Council of Europe, 2024b)).

За употребу ВИ система посебно су значајни принципи **минимизације података и ограничења сврхе**. Примена ових принципа подразумева да медијска организација не би требало да у ВИ систем уноси већи обим личних података него што је неопходно за конкретан новинарски задатак. Уколико се, на пример, ВИ користи за транскрипцију интервјуа или анализу докумената, није оправдано аутоматски обрађивати и податке који нису релевантни за ту сврху. На тај начин се смањује и могућност неовлашћеног откривања или даље употребе података (European Parliament & Council of the European Union, 2016).

Посебно важан је **члан 85 GDPR-а**, који захтева успостављање равнотеже између права на заштиту личних података и слободе изражавања и информисања, укључујући обраду у новинарске сврхе. Државама чланицама остављена је могућност да предвиде изузетке и дерогације од одређених правила GDPR-а када је то неопходно ради помирења ова два основна права (European Parliament & Council of the European Union, 2016).

Поред прописа о заштити података, за област медија значајан је и **Европски акт о слободи медија (European Media Freedom Act – EMFA)**, усвојен као Уредба (ЕУ) 2024/1083. Овај акт успоставља заједнички оквир за медијске услуге у Европској унији и усмерен је на јачање уређивачке независности, плурализма и заштите медија од неоправданог уплитања. Посебно је значајан за тему овог рада јер обухвата и заштиту новинарских извора и поверљиве комуникације, што је непосредно повезано са ризицима које дигиталне технологије и ВИ системи могу створити за безбедност извора (European Parliament & Council of the European Union, 2024).

На међународном нивоу значајан нормативни оквир има **Оквирна конвенција Савета Европе о вештачкој интелигенцији и људским правима, демократији и владавини права (CETS No. 225)**. Конвенција је отворена за потписивање 5. септембра 2024. године и представља први међународно правно обавезујући уговор који је посебно усмерен на обезбеђивање

усклађености активности повезаних са животним циклусом ВИ система са људским правима, демократијом и владавином права. Њен значај за медијски сектор огледа се у томе што поставља шири оквир за управљање ризицима, транспарентност и заштиту основних права приликом употребе ВИ система (Council of Europe, 2024a).

Уз правно обавезујуће инструменте, значајан међународни нормативни стандард представља и **Препорука UNESCO о етици вештачке интелигенције**. Иако није правно обавезујући инструмент попут закона или међународног уговора, она успоставља глобални етички оквир заснован на људским правима, људском достојанству, транспарентности, правичности, приватности, безбедности, одговорности и људском надзору. Посебно се наглашава да приватност и заштита података морају бити заштићене током целог животног циклуса ВИ система (UNESCO, 2021).

Поред правних норми, одговорна употреба вештачке интелигенције у новинарству захтева примену професионалних и етичких стандарда. Новинарска етика традиционално почива на принципима истинитости, тачности, одговорности, заштите приватности, поштовања људског достојанства и заштите извора. Увођење ВИ технологија не укида ове принципе, већ ствара потребу да се они примене на нове облике производње и дистрибуције медијског садржаја.

У том смислу посебно је значајан **Кодекс новинара и новинарки Србије**, у чијем је издању из 2025. године употреба вештачке интелигенције први пут изричито обухваћена посебним смерницама. Кодекс предвиђа да медији морају вештачку интелигенцију користити на транспарентан, одговоран и сразмеран начин и да су у целини одговорни за садржај објављен уз њену употребу. Такође се предвиђа обавештавање јавности када је медијски садржај креиран уз помоћ ВИ алата, као и јасно означавање случајева у којима је употреба ВИ значајно утицала на обраду новинарског садржаја.

Посебно је важно правило према којем садржај у чијем је креирању коришћена вештачка интелигенција мора остати под **уредничком контролом** и бити у складу са Кодексом. Овакво решење успоставља принцип према којем се одговорност за новинарски производ не може пренети на алгоритам или технолошког провајдера. Другим речима, чињеница да је одређени садржај генерисан или обрађен уз помоћ ВИ не ослобађа новинара и редакцију професионалне одговорности за његову тачност, законитост и етичку прихватљивост (Савет за штампу, 2025).

Сличан приступ заузима и **Савет Европе** у Смерницама о одговорној примени ВИ система у новинарству. Ове смернице обухватају различите фазе новинарског процеса – од одлуке о набавци и употреби ВИ система, преко њиховог укључивања у професионалне процедуре, до односа медија према публици и друштву. Основни принцип је да се технолошке иновације морају спроводити уз очување људских права, професионалне етике и уредничке контроле (Council of Europe, 2024г).

Смернице посебно наглашавају потребу за **проценом ризика пре увођења ВИ система**, одговарајућим процедурама приликом избора технологије и очувањем људског надзора над садржајем. Такав приступ је посебно важан када ВИ системи обрађују личне или поверљиве податке. Одлука о томе да ли се одређени документ, интервју, база података или други материјал сме обрадити путем ВИ система мора бити део професионалне и организационе процедуре, а не искључиво ствар индивидуалне процене новинара.

UNESCO такође наглашава принципе људског надзора, транспарентности, одговорности, безбедности и заштите приватности. У оквиру овог приступа ВИ системи не треба да потисну крајњу људску одговорност за одлуке које могу утицати на права и слободе појединаца (UNESCO, 2021).

Из наведених стандарда произлази да етичка употреба ВИ у новинарству подразумева најмање пет међусобно повезаних принципа: **транспарентност употребе ВИ**, уредничку

контролу, људски надзор, заштиту приватности и професионалну одговорност. Ови принципи су посебно важни у ситуацијама када се обрађују осетљиви подаци, када се користе системи персонализације или када ВИ учествује у процесу доношења уредничких одлука.

Упркос развоју правних и етичких стандарда, нормативни оквир за употребу ВИ у новинарству и даље се суочава са бројним изазовима. Основни проблем представља брзина технолошког развоја. Традиционални прописи о заштити података, приватности и медијима углавном су технолошки неутрални, што им омогућава да се примењују на нове технологије, али истовремено значи да не регулишу специфичне ризике сваке појединачне ВИ технологије.

Један од најзначајнијих изазова односи се на **утврђивање одговорности**. У класичном новинарском процесу релативно је јасно ко доноси одлуку о прикупљању, провери и објављивању информације. Код ВИ система у процес може бити укључен већи број субјеката: новинар, уредник, медијска организација, програмер, провајдер ВИ услуге и платформа преко које се садржај дистрибуира. Уколико ВИ систем обради личне податке на неочекиван начин или генерише садржај који нарушава нечија права, може бити сложено утврдити где се завршава одговорност технолошког провајдера, а где почиње одговорност медија.

Додатни проблем представља **нетранспарентност појединих ВИ система**. Новинарска редакција може користити модел чији начин функционисања није у потпуности познат крајњем кориснику. То отвара питања о томе на који начин систем обрађује унети материјал, колико дуго се подаци чувају, где се обрађују и да ли могу бити употребљени у друге сврхе. Код генеративне ВИ посебно је значајан проблем разграничења између материјала који је новинар унео у систем и резултата које систем производи на основу тог материјала.

Изазов представља и **прекогранична природа ВИ система**. Медијска организација може бити регистрована у једној држави, користити ВИ услугу компаније са седиштем у другој држави, док се обрада података врши на инфраструктури која се налази у више различитих јурисдикција. Такав модел компликује питања применљивог права, преноса података и надзора над обрадом.

Још једна празнина односи се на питање **деанонимизације и заштите новинарских извора**. Постојећи прописи о заштити података пружају значајну заштиту личним подацима, али способност савремених ВИ система да повезују велики број података ствара нове могућности за посредну идентификацију лица. То значи да традиционални приступ анонимизацији, који се заснива на уклањању директних идентификатора, у одређеним случајевима више није довољан.

Посебан изазов представља и **профилисање публике и аутоматизована персонализација садржаја**. Иако правни оквири препознају права појединаца у односу на аутоматизовану обраду и профилисање, технолошка сложеност савремених система отежава разумевање начина на који се појединачне препоруке формирају. У медијском окружењу то питање има и ширу друштвену димензију, јер алгоритамска персонализација не утиче само на приватност већ и на начин на који грађани приступају информацијама и формирају своје информативно окружење.

Због тога се будући нормативни приступ не може заснивати искључиво на усвајању нових прописа. Потребно је развијати **комбинацију правне регулације, професионалних етичких стандарда, интерних редакцијских правила, процене ризика и техничких мера заштите**. Овакав приступ одговара и ширем развоју међународног права у области ВИ. Оквирна конвенција Савета Европе о ВИ настоји да успостави технолојски неутралан оквир који може одговорити и на будуће облике ризика, управо зато што се технологије и њихове примене брзо мењају (Council of Europe, 2024a).

У том смислу, регулација ВИ у новинарству треба да тежи успостављању равнотеже између две групе интереса. Са једне стране, неопходно је очувати слободу изражавања, право јавности да буде информисана и могућност новинара да користе технологије које унапређују

истраживачки и аналитички рад. Са друге стране, неопходно је обезбедити да технолошка ефикасност не буде остварена на рачун приватности грађана, поверљивости извора, људског достојанства и професионалне одговорности медија. Све наведено показује да савремени правни и етички оквир не треба посматрати као препреку употреби вештачке интелигенције у новинарству, већ као механизам за њено одговорно увођење. Основни захтев није да се ВИ технологије искључе из новинарског процеса, већ да се њихова примена подреди принципима законитости, неопходности, сразмерности, транспарентности, заштите приватности, уредничке независности и људске одговорности.

ЗАКЉУЧАК

Вештачка интелигенција више није технологија која тек треба да пронађе своје место у новинарству. Она је већ постала део новинарског процеса – од претраживања и обраде података, транскрипције и превођења, до генерисања, персонализације и дистрибуције медијског садржаја. Питање које се данас поставља, зато, више није да ли ће редакције користити вештачку интелигенцију, већ **под којим условима ће је користити и ко ће сносити последице када њена употреба угрози права грађана?** У том контексту, кључни изазов није у самој употреби вештачке интелигенције, већ у начину на који се она интегрише у новинарски процес. Ефикасност коју ВИ пружа мора бити праћена људском контролом, провером информација и јасно утврђеном одговорношћу за коначни садржај. Посебну пажњу захтевају заштита личних података, поверљивост извора и транспарентност алгоритамске обраде, због чега технолошки развој мора бити праћен одговарајућим правним и професионалним стандардима. ВИ тако може представљати средство за унапређење новинарског рада, а не фактор који нарушава његову основну друштвену функцију. Будућа примена вештачке интелигенције у новинарству захтеваће истовремено уважавање технолошких могућности и ограничења која произлазе из заштите људских права, професионалне етике и важећег правног оквира. Посебан значај имаће очување људског надзора над процесима у којима се користе ВИ системи, као и одговорно управљање личним и поверљивим подацима. У том смислу, успешна интеграција вештачке интелигенције у новинарску праксу не подразумева само повећање ефикасности производње садржаја, већ и очување професионалних стандарда, заштите приватности, поузданости информација и поверења јавности у медије.

РЕФЕРЕНЦЕ

European Parliament & Council of the European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.

European Parliament & Council of the European Union (2024). *Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act)*. Official Journal of the European Union, L 2024/1083.

Закон о заштити података о личности (2018). *Службени гласник Републике Србије*, бр. 87/2018.

Jones, B., & Galanos, V. (2024). *Generative AI and journalism: Mapping the risk landscape*. University of Edinburgh. <https://doi.org/10.5281/zenodo.14968182>

Lopezosa, C., Pérez-Montoro, M., & Rey Martín, C. (2024). The use of artificial intelligence in newsrooms: Proposals and limitations. *Revista de Comunicación*, 23(1), 279–293. <https://doi.org/10.26441/RC23.1-2024-3309>

Newman, N. (2025). *Overview and key findings of the 2025 Digital News Report*. Reuters Institute for the Study of Journalism, University of Oxford.

Newman, N., & Cherubini, F. (2025). *Journalism, media, and technology trends and predictions 2025*. Reuters Institute for the Study of Journalism, University of Oxford. <https://doi.org/10.60625/risj-vte1-x706>

Ross Arguedas, A. (2025). *How audiences think about news personalisation in the AI era*. Reuters Institute for the Study of Journalism, University of Oxford.

Савет за штампу (2025). *Кодекс новинара и новинарки Србије*. Савет за штампу.

Simon, F. M., Nielsen, R. K., & Fletcher, R. (2025). *Generative AI and news report 2025: How people think about AI's role in journalism and society*. Reuters Institute for the Study of Journalism, University of Oxford. <https://doi.org/10.60625/risj-5bjv-yt69>

Sonni, A. F., Hafied, H., Irwanto, I., & Latuheru, R. (2024). Digital newsroom transformation: A systematic review of the impact of artificial intelligence on journalistic practices, news narratives, and ethical challenges. *Journalism and Media*, 5(4), 1554–1570. <https://doi.org/10.3390/journalmedia5040097>

Thurman, N., Thäsler-Kordonouri, S., & Fletcher, R. (2025). *AI adoption by UK journalists and their newsrooms: Surveying applications, approaches, and attitudes*. Reuters Institute for the Study of Journalism, University of Oxford. <https://doi.org/10.60625/risj-ea11-q402>

UNESCO (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.

Cools, H., & Diakopoulos, N. (2024). Uses of generative AI in the newsroom: Mapping journalists' perceptions of perils and possibilities. *Journalism Practice*, 18(4), 878–896. <https://doi.org/10.1080/17512786.2024.2394558>

Council of Europe (2024a). *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225)*. Council of Europe.

Council of Europe (2024b). *Potential amendments to Serbia's Data Protection Law with emphasis on Freedom of Expression discussed with local actors*. Council of Europe, Horizontal Facility. Council of Europe (2024в). *Strengthening data protection standards in Serbia*. Council of Europe, Horizontal Facility. Council of Europe, Steering Committee on Media and Information Society (2024г). *Guidelines on the responsible implementation of artificial intelligence systems in journalism*. Council of Europe.

МЕДИЈСКА РЕПРЕЗЕНТАЦИЈА И ДИГИТАЛИЗАЦИЈА АРХИТЕКТОНСКОГ НАСЛЕЂА НАЦИОНАЛНИХ МАЊИНА ВОЈВОДИНЕ И САВРЕМЕНЕ ИНТЕРПОЛАЦИЈЕ

Катарина Стојановић¹

Сажетак

Формирање специфичних архитектонских израза међу националним мањинама Војводине дуго је посматрано изоловано од савремених комуникационих токова. Међутим, улога масовних и нових дигиталних медија постаје кључна у процесу документације, валоризације и заштите мултикултуралног панонског стила, који је настајао кроз дијалог средњоевропских праваца (барока, класицизма, сецесије) и традиционалних руралних техника. Савремени медијски дискурс често маргинализује градитељско наслеђе мањинских заједница (Мађара, Словака, Русина, Румуна, Немаца), чиме се убрзава губитак регионалног мултиетничког идентитета. Сврха овог рада је да истражи како се кроз историјски метод, али и савремене мултимедијалне платформе и дигиталне медије, може извршити типизација мање познатих објеката и понудити модел за њихову савремену архитектонску интерполацију. Упоредном анализом истражује се утицај јавних медијских кампања и нових носилаца информација на перцепцију мањинске архитектуре. У контексту изолованих и демографски угрожених војвођанских села, нови медији и дигитални архиви препознати су као последњи инструмент за трансмисију аутентичних вредности пре њиховог физичког нестанка. Анализом планова, литературе и интернет-медија потврђује се почетна хипотеза: док дигитална заједница препознаје панонске архитектонске типове као универзалне за овај простор, специфични медијски наративи сваке заједнице истичу подтипове условљене културом и етничким пореклом.

Кључне речи: Дигитални медији, Архитектонско наслеђе, Националне мањине, Војводина, Интерполација

¹ Факултет савремених уметности, Београд, Универзитет Привредна академија у Новом Саду; Грађевински факултет Суботица, Универзитет у Новом Саду, Србија
е-маил: katarina.stojanovic@fimek.edu.rs

УВОД

Истраживање просторних односа данас се не може посматрати одвојено од информационе сфере и медијског простора који те односе уобличава. Анализирајући друштвено-политички оквир Војводине у 19. и 20. веку, закључујемо да је мултикултурална архитектура регије одувек зависила од канала комуникације и тадашњих штампаних медија који су ширили средњоевропске архитектонске трендове. Тренутно, савремени глобални стилови у архитектури вођени су агилношћу капитала и шире се кроз планетарне масовне медије, агресивно пропагирајући урбану униформност. Локални медијски наративи углавном пате од индоленције према специфичности-ма мањинских заједница.

Идентификација и медијска промоција карактеристичних типологија народног грађитељства представља прву одбрану у стратешком планирању и очувању идентитета у новом миленијуму. Уколико архитектура националних мањина није видљива у дигиталним и масовним медијима, она практично престаје да постоји у свести шире јавности, што олакшава њено физичко девастирање у актуелним урбаним токовима. Стога, овај рад ставља фокус на важност мултимедијалног каталогизовања објеката Бачке, Баната и Срема, указујући на потенцијал који медијске технологије имају у архитектонском пројектовању и заштити. Репрезентативне примере регионалне сецесије и историцизма у контексту културне комуникације изучавали су Кадијевић (2007) и (Duranci, 2005).

ИСТОРИЈСКИ КОНТЕКСТ И ПРЕДУСЛОВИ СТВАРАЊА АРХИТЕКТУРЕ НАЦИОНАЛНИХ МАЊИНА

Појава посебних стилских слојева у архитектури националних мањина у Војводини била је условљена не само државном колонизацијом већ и развојем раних комуникационих канала. Богатији мањински слојеви и њихове институције (попут словачких, мађарских или румунских културних матица) усвајали су средњоевропски архитектонски језик, преобликујући војвођанска села у ортогоналне урбане структуре насупрот балканско-оријенталном контексту јужнијих крајева. Веома важну улогу у овој комуникацији имали су путујући мајстори и градитељи који су служили као живи „медији” за трансмисију знања са севера. Сакрална архитектура католика, протестаната и гркокатолика у Војводини постала је предмет првих медијских критика и дебата у тадашњој периодици, што је јачало идентитет нове мултиетничке буржоазије. Архитектура институција (банака, културних домова) јасно је медијски поручивала јавности о економској снази мањинских заједница. Недавне анализе истичу да је данас за очување ових објеката неопходна њихова поновна валоризација у новим локалним медијима (Siladi, 2021), како би се спречио дисконтинуитет настао услед честих историјских турбуленција (Nestorović, 2014).

Данас, у ери четврте индустријске револуције, дигитални медији и мултимедијални архиви постају примарни чувари ове баштине. Традиционална кућа од набоја или бондрука, као регионални градитељски стандард, добија нову форму постојања кроз 3Д ласерско скенирање, виртуелну реалност (VR) и дигиталне базе података. Као што је приказано у модерним медијским

објавама и студијама о панонској кући (Dukanović, 2019), дигитализација градитељског нацрта омогућава да се уочи како су различите мањинске заједнице на истој географској основи развијале специфичне естетске нијансе на забатима и тремовима. Разумевање ових модела кроз дигиталне медије омогућава савременим пројектантима да креирају структуралне моделе за будућност који су у складу са одрживим развојем (Živković, Kurtović-Folić, Jovanović, Kondić, Mitković, 2016).

КРИТЕРИЈУМИ И ТИПОЛОШКА АНАЛИЗА

Увођење појма медија захтева проширење стандардних типолошких критеријума (време, локација, материјал, конструкција) на нове визуелне и информационе критеријуме. То су: медијска видљивост објекта, степен његове дигиталне документованости, те наративни потенцијал у контексту заједнице којој припада. Ретко очувани објекти мањинске народне архитектуре који поседују висок ниво занатске чистоће и лепоте представљају идеалан медијски садржај за промоцију историјске аутентичности (Živković, 2011).

Проблем брзог нестајања ових кућа у целој Србији управо је последица изостанка из медијске сфере - објекти који нису уврштени у јавне дигиталне каталоге лакше се руше услед мањка правних последица и непознавања њихове вредности (Jukileto, 2002). Масовна изградња на штету пољопривредног земљишта праћена је потпуним медијским муком о деструкцији баштине националних мањина. На супрот томе, монументални објекти попут мађарских грађанских касина, словачких народних домова или русинских седишта у Суботици, Сомбору или Зрењанину, одувек су имали већу медијску пажњу. Архитектонска естетика сецесијских јавних палата, коју су пројектовали Комор, Јакоб или Табаковић, данас је главни визуелни медијски бренд градова попут Суботице, о чему сведоче обимне мултимедијалне и монографске студије (Aladžić et al., 2004]).



Слика 1. Градска кућа у Суботици као пример врхунске мађарске сецесије је доминанта на многим порталима

Извор: https://subotica.ls.gov.rs/web/wp-content/uploads/2022/06/14811_38.jpg?x23492

Овакав начин архивирања сакралних и профилних објеката (попут храмова у Ковачици или Дебељачи) кроз телевизијске репортаже и специјализоване архитектонске сајтове доприноси њиховој материјалној заштити. Куће које на уличним забатима имају декоративне барокне лукове, канелуре или панонске тремове (ганг), захваљујући медијској пажњи добијају статус баштине, чиме се мотивише локално становништво на рестаурацију.

РЕЗУЛТАТИ И ДИСКУСИЈА

Досадашња истраживања која су обухватала објекте са краја 19. и почетка 20. века показују да укрштање архитектонске историје и теорије медија даје потпуно нове резултате. Прелаз са класицизма на романтизам и сецесију у Војводини није био само естетски покрет већ медијска револуција у начину на који су етничке групе комуницирале свој идентитет према већинском становништву и администрацији. Спајање модерних токова са традицијом панонског троделног модела становања (предна изба, питвор, задна изба), који је заједнички за Словаци, Румуне и Мађаре, визуелно показује висок степен регионалне кохезије (Medved, 2021). Инкорпорација мањинских тема у уско специјализоване медије онемогућава да ово наслеђе уђе у ширу јавну свест као универзална вредност Војводине.

УПОРИШТЕ У НАРОДНОЈ АРХИТЕКТУРИ КРОЗ НОВЕ МЕДИЈЕ

Поређење мање познатих руралних кућа на територији Војводине показује занимљиву појаву: дигитални медији данас деконструишу географске и културне митове. Кроз упоредне интернет-базе података јасно се види да одређени грађевински типови настају као одговор на услове средине (близина река, влажност тла, панонска ветровитост), док подтипови носе у себи информациони код конкретне народне (Milohnić, Švob-Đokić, 2011).



Слика 2. Замак у Руском Крстуру је препознатљив објекат русинске архитектуре на регионалним туристичким порталима и сајтовима који прате заштиту споменика културе

Извор: <https://turizamkula.rs/wp-content/uploads/2018/05/zamak-muzej-i-skola.jpg>



Слика 3. Символи традиције Словака у Војводини, завичајна кућа споменик културе од изузетног значаја и најстарија кућа у Бачком Петровцу
Извор: <https://www.backipetrovac.rs/images/muzej-mnjac.jpg>

Ови примери потврђују да савремени електронски медији могу послужити као одличан извор за компаративне научне студије, чинећи лако доступним материјал који би иначе због удаљености и физичке деградације остао затворен за истраживаче.

САВРЕМЕНЕ МЕДИЈСКЕ ТЕХНОЛОГИЈЕ И ИНТЕРПОЛАЦИЈА У РЕГИОНАЛНОМ СТИЛУ

Урбани морфолози истичу да је „разумевање места” и његовог идентитета услов за правилно просторно управљање (Samuels, 2010). Данас се то разумевање значајно убрзава кроз нове медијске алате - рачунарске симулације, BIM технологију и дигитално пројектовање. Савремени архитекти могу кроз медијски посредовану традицију да црпе инспирацију из фолклора националних мањина Војводине. Физичко наслеђе и људски развој не могу се раздвајати, а улога медијских кампања је да подигну друштвену свест о потреби конзервације (Mutal, 2011).



Слика 4. Савремени редизајн традиционалног типа војвођанске куће
Извор: <https://www.daibau.rs/showfile.php?uuid=302821d3150aae2bf2d5c0be3109b976ef76fea1>

Овакви примери показују моћ архитектуре када се удружи са дигиталним медијима: објекти који успешно спајају мањинску традицију и савремени дизајн постају вирални у глобалном информационом простору. То директно утиче на промену локалне парадигме и доказује да панонски народни стил није превазиђен, већ да у синергији са модерним медијским изразом представља врхунски архитектонски производ који чува мултиетнички дух регије.

ЗАКЉУЧЦИ

Дух једног места гради се кроз материјалне аспекте али се трансмитује кроз медије комуникације. Архитектонско пројектовање даје простору карактер (Norberg-Schulz, 1978), док му медији обезбеђују трајање у колективној меморији. Специфичне типологије народне и грађанске архитектуре националних мањина у Војводини, које су анализиране у овом раду, доказују да се одговори на изазове савремене глобализације налазе у сопственом мултикултуралном наслеђу. Споменици културе су материјалне чињенице које је тешко замућити (Radović, 2005), али без њиховог присуства у савременом медијском и дигиталном простору, они су осуђени на тихи заборав и физичко пропадање. Повезивање архитектонске генезе (Kurtović-Folić, 2015) са медијским технологијама отвара нове хоризонте за будућност просторног планирања у Војводини. Један од главних закључака овог рада јесте да савремена оптимизација пројектовања и интерполације мора користити нове медије за едукацију, промоцију и документацију сваког специфичног мултиетничког простора појединачно. Само кроз активну медијску репрезентацију, архитектонски опус националних мањина Војводине може постати равноправан део савремених светских трендова, чувајући свој локални идентитет од нестанка.

ЗАХВАЛНИЦА

Овај рад је подржан од стране Министарство за људска и мањинска права и друштвени дијалог, Републике Србије, у оквиру реализације пројекта под називом: „Архитектура као идентитет: Промоција архитектонског наслеђа националних мањина Војводине”, додељеног на конкурс за средства из Буџетског фонда за националне мањине у 2026. години за програме и пројекте из области културе.

РЕФЕРЕНЦЕ

Aladžić, V., Duranci, B., & Grlica, M. (2004). *Secesija u Subotici - A szecesszió Szabadkán*. Međuopštinski zavod za zaštitu spomenika kulture.

Dukanović, M. (2019). *Bioklimatska arhitektura tradicionalnih vojvođanskih kuća*. Fakultet tehničkih nauka.

Duranci, B. (2005). *Arhitektura secesije u Subotici*. Međuopštinski zavod za zaštitu spomenika kulture.

Jukileto, J. (2002). Planiranje naselja i konzervacija. *Glasnik DK*, (26), 24–26.

Kadijević, A. (2007). *Jedan vek traženja nacionalnog stila u srpskoj arhitekturi* (sredina XIX – sredina XX veka). Građevinska knjiga.

Kurtović-Folić, N. (2014). *Kulturno nasleđe kao arhitektonski kontekst*. FTN.

Maroši, M. (2018). Arhitektura historicizma i secesije u Subotici. *Zbornik radova Fakulteta tehničkih nauka*, 3, 110–115.

Medveđ, T. (2021). Narodna arhitektura Slovaka u Vojvodini. U *Kulturno nasleđe vojvođanskih Slovaka*. Zavod za kulturu vojvođanskih Slovaka.

Milohnić, A., & Švob-Đokići, N. (2011). *Cultural identity politics in the (post-)transitional societies*. Institute for International Relations.

Mutal, S. S. (2011). The future of historic cities: A practitioner's experience. *Historic Environment*, 23, 61–65.

Nestorović, B. (2014). *Arhitektura Srbije u XIX veku*. Art Pres.

Norberg-Schulz, C. (1978). Building in old settings as a problem of place. U *New building in old settings*, State Museum for Applied Arts, Munich; 11-13.

Radović, R. (2005). *Novi vrt i stari kavez*. Stylos.

Samuels, I. (2010). Understanding place. *Urban Morphology*, 14(2), 121–123.

Silađi, M. (2021). Graditeljsko nasleđe manjinskih zajednica Novog Sada. *Zbornik radova Fakulteta tehničkih nauka u Novom Sadu*, 5, 182–187.

Živković, M., Kurtović-Folić, N., Jovanović, G., Kondić, S., & Mitković, M. (2016). Current strategies of urban and architectural conversion as a result of increased housing demands. *Tehnički vjesnik*, 23(2), 561–568.

Živković, N. (2011). Gročanske kuće – paradigma vremena. *Nasleđe*, 12, 267–279.

ДИГИТАЛНИ МЕДИЈИ И МУЗИЧКА ИНДУСТРИЈА: ЗАШТИТА ПРИВАТНОСТИ КОРИСНИКА НА СТРИМИНГ ПЛАТФОРМАМА

Николета Дојчиновић¹

Сажетак

Развој дигиталних медија у последњим деценијама значајно је променио музичку индустрију, начине дистрибуције и односе између музичких садржаја, платформи и публике. Стриминг платформе постале су један од најзначајнијих модела приступа музици, а њихов раст прати све већи утицај алгоритама који обликују избор, препоруке и видљивост музичких садржаја. Истовремено, њихово функционисање заснива се на прикупљању и обради великих количина података о корисницима, што отвара важна питања у вези са приватношћу, сигурношћу података и дигиталним правима. Овај рад истражује улогу стриминг платформи као савремених дигиталних медија и тражи одговор на питање како успоставити равнотежу између персонализације музичких садржаја, која се заснива на алгоритамској обради корисничких података, и права корисника на приватност. Посебна пажња посвећена је транспарентности дигиталних платформи, начинима коришћења корисничких података и изазовима који настају у односу између технолошког развоја и заштите дигиталних права. У раду ће бити размотрено и место музичке индустрије у Србији у оквиру глобалног дигиталног медијског окружења, са освртом на утицај стриминг платформи на доступност музичких садржаја и положај корисника. Циљ рада је да укаже на потребу успостављања равнотеже између развоја дигиталних медија, нових модела дистрибуције музике и одговорног односа према подацима корисника.

Кључне речи: дигитални медији, музичка индустрија, стриминг платформе, заштита приватности, лични подаци

¹ Музичка продукција Радио-телевизије Србија, Београд, Србија
e-mail: nikoletadojcinovic@gmail.com

УВОД

Појавом и развојем дигиталних медија традиционални модели музичке индустрије и однос између аутора, издавача, дистрибутера и публике постепено се мењао током последњих деценија. Музика је постала доступнија у сваком тренутку и са различитих уређаја. Посебно значајна, можда и најзначајнија, јесте појава стриминг (streaming) платформи које су постале један од доминантних начина приступа музичким садржајима посредством интернета. Овим музика све мање постаје производ који се купује и поседује, физички или дигитални снимак, а све више услуга којој се приступа у складу са сопственим потребама и навикама.

Подаци глобалне музичке индустрије потврђују значај стриминга и његов убрзан развој. Према извештају IFPI Global Music Report 2026, укупни приходи светске индустрије снимљене музике у 2025. години достигли су 31,7 милијарду америчких долара, уз раст од 6,4% у односу на претходну годину. Приходи од стриминга премашили су 22 милијарде долара и чинили 69,6% укупних прихода од снимљене музике, док је број корисника плаћених претплатничких стриминг сервиса достигао 837 милиона. Ови показатељи потврђују да стриминг више није само један од алтернативних начина дистрибуције музике, већ један од кључних сегмената савременог музичког и дигиталног медијског окружења.

Иако IFPI у јавно доступном делу извештаја не издваја детаљне показатеље за Србију, доступни подаци о појединачним платформама показују присуство и раст значаја стриминг сервиса и на домаћем тржишту. Према подацима компаније Sensor Tower, у четвртном кварталу 2025. године недељни приходи апликације Spotify у Србији кретали су се приближно између 1.300 и 1.600 америчких долара, док су преузимања апликације у једној недељи почетком децембра достигла око 7.600. У истом периоду YouTube Music је забележио врхунац од око 2.300 преузимања у једној недељи. Ови подаци не представљају укупну вредност српског тржишта музичког стриминга, али указују на присуство и коришћење глобалних стриминг платформи у Србији. Према подацима Statista Market Insights, процењена просечна годишња потрошња по кориснику у Србији на дигитална преузимања музике и претплате на музичке стриминг сервисе у 2025. години износила је 13,76 америчких долара, док је светски просек био 35,14 долара.

Стриминг платформе путем алгоритама анализирају различите облике интеракције корисника са платформом и на основу тих података креирају препоруке, персонализоване листе и друге облике прилагођеног садржаја. На тај начин корисничко искуство постаје индивидуализовано, али се истовремено велики број података о кориснику прикупља и обрађује.

Када је реч о томе које податке платформе прикупљају, најчешће се разликују подаци неопходни за отварање и одржавање налога (идентификациони подаци, подаци о претплати и плаћању), технички подаци о уређају и коришћењу апликације, подаци о локацији у мери у којој су укључени у подешавања услуге, као и подаци о самом понашању корисника током слушања – које песме слуша, колико дуго, шта прескаче, шта поново слуша и које листе креира. Сврхе обраде нису јединствене: део обраде је неопходан за пружање основне услуге (наплата, техничко функционисање, безбедност налога), други део служи персонализацији садржаја, а трећи део, посебно код бесплатних, огласно финансираних облика коришћења, повезан је с монетизацијом, односно креирањем корисничких профила ради циљаног оглашавања и извештавања према рекламодавцима.

У пракси, ниво информисаности корисника о овим сврхама варира: платформе формално објављују политике приватности и услове коришћења, али је њихова дужина и правна сложеност често препрека стварном разумевању. Могућност контроле такође постоји, у виду

подешавања приватности, права приступа и брисања података или искључивања појединих облика персонализације, али је она у пракси ограничена обимом информација које су кориснику на располагању у тренутку доношења одлуке.

ДИГИТАЛНА ТРАНСФОРМАЦИЈА МУЗИЧКЕ ИНДУСТРИЈЕ

Трансформација музичке индустрије под утицајем дигиталних медија одвијала се постепено јер су се мењали технологија, начини производње и дистрибуције, пословни модели и односи између учесника у музичком систему. Дигитализација је истовремено променила и положај публике: од претежно пасивног примаоца музичког садржаја, слушалац је постао активни корисник који самостално бира, претражује, организује и дели музички садржај. Овај помак прати ширу тенденцију у теорији медија да се публика посматра као активан учесник, а не само крајњи прималац порука. Још је Тофлер увео појам „просумера”, корисника који истовремено троши и делимично обликује садржај који користи, а каснија истраживања дигиталних медија овај концепт даље развијају описујући корисника као учесника у обликовању сопственог медијског искуства, а не само као пасивног слушаоца. Једна од последњих теорија које се бави односом публике и медија је теорија Клеја Ширкија која говори о „смрти или крају публике”, у смислу да публика није више само публика, посматрач, прималац порука, већ и активни учесник, креатор садржаја.

Традиционална музичка индустрија била је заснована на физичким носачима звука и релативно јасно дефинисаном ланцу производње и дистрибуције. Издавачка кућа, дистрибутер, продавница и медији имали су посредничку улогу између аутора и публике. У дигиталном окружењу тај модел је постао знатно флексибилнији. Музички садржај више није неопходно повезан са физичким носачем, а његова дистрибуција може се одвијати непосредно, глобално и готово тренутно.

Појава дигиталних аудио формата и могућност њиховог преноса путем мреже довели су до настанка нових начина размене и приступа музици. У почетку су значајан део те трансформације представљали сервиси за преузимање музике и peer-to-peer (P2P) мреже², када се увидело да се садржај може одвојити од физичког носача и дистрибуирати у потпуно новом медијском окружењу. Већ тада су отворена бројна питања у вези са ауторским правима и контролом дистрибуције.

Следећа фаза донела је прелазак са модела преузимања на модел приступа садржају. Уместо да корисник купује појединачне снимке и чува их на сопственом уређају, дигитални сервиси омогућили су приступ великим музичким каталозима путем интернета. Овим приход више није нужно био заснован на продаји појединачног физичког или дигиталног производа, већ све више на претплати, оглашавању и другим облицима монетизације.

² Развој се одвијао у неколико препознатљивих периода: крај 1990-их и почетак 2000-их обележили су сервиси за неовлашћену размену датотека попут *Napster*-а (покренут 1999, угашен 2001. услед судских спорова) и мреже попут *LimeWire* и *Kazaa*; период од 2003. године донео је успон легалних сервиса за куповину појединачних снимака, попут *iTunes Music Store*-а, који је покренут у априлу 2003. године; од 2008. године, оснивањем сервиса *Spotify* у Шведској, почиње развој модела приступа садржају путем стриминга и претплате, док је ширење сервиса на тржиште САД уследило 2011. године. Током друге половине 2010-их стриминг постепено постаје доминантан модел приступа музици на глобалном нивоу, а 2017. године постаје и највећи појединачни извор прихода у глобалној индустрији снимљене музике.

Управо ту долази до промене улоге дигиталних платформи. У традиционалним медијима избор музике у великој мери био је у рукама уредника, програмских шема и професионалних посредника. У дигиталном окружењу део те функције преузимају алгоритамски системи. Они могу да анализирају карактеристике музичког садржаја, али и податке о начину на који корисници користе платформу, како би одредили који ће садржај бити приказан, препоручен или постављен у одређени контекст.

На тај начин дигитални медији нису само променили начин на који се музика дистрибуира већ и начин на који се она открива. Раније је пут до нове музике често водио преко радиостанице, телевизијске емисије, музичке критике, продавнице плоча или препоруке другог слушаоца. Данас тај пут све чешће почиње на дигиталној платформи, у претрази, препорученој листи, аутоматски генерисаној листи песама или садржају који се кориснику приказује на основу његових претходних избора.

Слушање музике истовремено постаје и извор података о корисничким навикама. Тиме се ствара повезаност између слушања, прикупљања података и персонализације садржаја, што представља једну од кључних карактеристика савременог дигиталног музичког окружења.

СТРИМИНГ ПЛАТФОРМЕ, АЛГОРИТМИ И ПЕРСОНАЛИЗАЦИЈА

Стриминг платформе, као један од најзначајнијих резултата дигиталне трансформације музичке индустрије, обично функционишу кроз комбинацију претплатничког и огласног модела. Код претплатничког модела корисник плаћа месечну или годишњу накнаду за приступ садржају и одређеним функцијама сервиса. Код модела који се финансира оглашавањем приступ садржају може бити бесплатан, али је корисник изложен огласима, а платформа остварује приход од оглашивача. Постоје и комбиновани модели, као и различити нивои услуге.

То мења и начин вредновања музике. Број слушања, дужина слушања, број корисника, активност публике и други показатељи постају важни за процену успешности одређеног садржаја. Тиме је платформа истовремено дистрибутер, претраживач, каталог, препоручивач и посредник између корисника и музичког садржаја.

Сам процес прикупљања података тече у пет корака: генерисање догађаја³ → пренос података⁴ → прихват и сортирање⁵ → складиштење⁶ → обрада алгоритама⁷.

³ Телеметрија: Сваки клик, покретање или заустављање песме/видеа покреће такозвани *event* (догађај).

⁴ *API* сервери: Преко интернет везе, апликација шаље те податке назад на централне сервере компаније путем *API*-ја (*Application Programming Interface*). Ово се дешава у размацима од неколико милисекунди до неколико минута како вам се не би трошила батерија.

⁵ *Data Pipelines*: сервис користе моћне системе за управљање великим количинама података (као што су *Apache Kafka* или *AWS Kinesis*). Ови системи раде као огромне дигиталне „Сортирнице” које прихватају неструктуриран прилив информација и одмах их разврставају (нпр. технички логови иду на једну страну, а историја слушања на другу).

⁶ *Data Lakes*: Сортирани подаци се чувају или као краткорочно складиште (за тренутне потребе - нпр. да апликација памти где сте стали са гледањем филма ако вам пукне веза) или као дугорочно складиште (*Data Lakes/Warehouses*) у облаку (*Cloud*) где се чува комплетна историја вашег понашања од дана када сте направили профил.

⁷ Машинско учење: Системи вештачке интелигенције пролазе кроз складиштене податке појединца и упоређују их са подацима милиона других корисника. Машинско учење тада ажурира „кориснички профил укуса” појединца и моментално враћа назад у апликацију корисника нове препоруке, персонализоване листе или циљане рекламе.

Стварање персонализованог медијског окружења видљиво је, на пример, у функцијама аутоматски генерисаних недељних и дневних листа које велике платформе нуде својим корисницима, а које се у потпуности формирају на основу претходног понашања слушаоца. Овде се отвара простор за алгоритамску селекцију. Платформа мора да обради огромну количину садржаја и да кориснику понуди избор који ће за њега бити релевантан. Без алгоритамских система било би тешко ефикасно управљати каталогом који садржи милионе снимака. Међутим, да би систем био што персонализованiji, неопходна је већа количина информација која се користи за његово функционисање. Корисничко слушање тако постаје део механизма којим се обликује његово будуће музичко искуство.

Препоруке су засноване на различитим врстама информација – претходно слушани садржаји, учесталост слушања, прескакање песама, претраге, креиране листе, омиљени извођачи, време коришћења сервиса и интеракције са различитим функцијама платформе. Систем може узимати у обзир и карактеристике самог музичког садржаја, као што су жанр, темпо, структура, извођач или сличност са другим песмама.

На основу тако прикупљених информација алгоритам покушава да претпостави шта би корисник желео да слуша. Персонализација зато није само техничко питање већ механизам који непосредно утиче на медијско искуство, али има и значајну економску функцију.

Код сервиса који се финансирају оглашавањем, подаци о навикама и интересовањима могу се користити за прецизније усмеравање рекламних садржаја, док код претплатничких модела персонализација може допринети задовољству корисника и његовом задржавању на платформи. На тај начин подаци о корисничком понашању постају важан економски ресурс, јер њихова анализа омогућава платформи да оптимизује понуду и повећа могућност остваривања прихода. Корисник може добити препоруку за извођача за којег раније није чуо или за жанр који није активно претраживао. За музичку индустрију то може представљати важан канал промоције и откривања нових аутора и извођача.

Истовремено, алгоритамска препорука није неутрална у потпуности. Оно што корисник види и чује зависи од начина на који је систем конструисан. Поставља се питање да ли алгоритам само препознаје постојеће укусе или их делимично и обликује. Ако корисник стално добија сличне садржаје, могуће је да се његов избор постепено сузи на одређени круг жанрова, извођача или стилова. Овде се појављује феномен такозваног „филтерског межура”, концепт који је у ширу употребу увео Паризер, а који у музичком контексту значи да корисник све више добија садржај сличан ономе који је већ користио. У музичком контексту то може значити већу удобност и релевантност препорука, али и мању изложеност другачијим музичким садржајима, што може довести и до засићења корисника.

Алгоритамска персонализација зато има и културну димензију. Ако платформа има значајну улогу у томе шта корисник открива, она посредно утиче и на видљивост одређених извођача, жанрова и музичких продукција. То је посебно значајно за мање музичке сцене и локалне садржаје, који се такмиче са огромном количином глобалне музичке продукције.

ПОДАЦИ КОРИСНИКА И ПИТАЊЕ ПРИВАТНОСТИ

Коришћење стриминг платформе оставља дигитални траг, те корисник не пружа платформи само информацију о томе коју песму жели да слуша већ, кроз своје понашање, ствара низ података који могу бити анализирани и повезивани.

Подаци могу обухватати основне информације потребне за креирање корисничког налога, податке о претплати и плаћању, податке о уређају, техничке информације, локацијске податке, у зависности од подешавања и услуге, као и податке о начину коришћења платформе. За персонализацију су посебно значајни подаци о слушању: шта је корисник слушао, колико дуго, шта је прескочио, шта је поново слушао, које извођаче претражује и које листе креира.

Наизглед безазлена информација о музичком укусу, када се комбинује са другим подацима, може открити много више о особи. Музички избори могу бити повезани са узрастом, животним стилем, расположењем, културним интересовањима или другим карактеристикама корисника. Због тога питање приватности не треба свести само на заштиту имена, адресе електронске поште или података о плаћању. Важно је и питање шта платформа може да закључи о кориснику на основу његовог понашања.

Посебан проблем представља профилисање које подразумева обраду података ради процене или предвиђања одређених карактеристика, интересовања или понашања појединца. У случају музичких платформи оно може имати легитимну функцију – омогућавање персонализованих препорука – али истовремено ствара потребу за јасним информисањем корисника о начину на који се таква обрада спроводи.

Корисник би требало да зна које се категорије података обрађују, у које сврхе, колико дуго се чувају и да ли се прослеђују другим субјектима. Посебно је важно да услови коришћења и политике приватности буду разумљиви, а не само формално доступни.

Проблем настаје када корисник прихвата услове коришћења без стварног разумевања последица. Дугачки и сложени документи могу довести до ситуације у којој постоји формална сагласност, али ограничено стварно разумевање начина обраде података. Зато транспарентност представља један од кључних принципа одговорног дигиталног медијског окружења. Корисник не би требало да буде сведен на објекат алгоритајске анализе, већ мора имати могућност да разуме и, у оквиру права која му закон гарантује, контролише начин на који се његови подаци користе.

Питање је, међутим, у којој мери ова права постоје само на формалном нивоу, а у којој мери корисник заиста може да утиче на обраду својих података. Због тога је неопходно размотрити правне оквире који регулишу прикупљање, обраду, чување и пренос података, као и права која корисницима стоје на располагању. У том контексту посебан значај имају Општа уредба о заштити података Европске уније (GDPR), прописи Сједињених Америчких Држава, пре свега Калифорнијски закон о приватности потрошача (CCPA/CPRA), као и Закон о заштити података о личности Републике Србије.

ПРАВНИ ОКВИРИ ЗАШТИТЕ ПОДАТАКА

Питање заштите приватности на стриминг платформама део је ширег система заштите података о личности. Поред података неопходних за отварање налога и наплату услуге, платформе могу прикупљати податке о уређају, претрагама, слушаним садржајима и интеракцијама са услугом, што омогућава анализу и профилисање корисника. Зато је важно не само како се подаци штите, већ и под којим условима се прикупљају, обрађују, чувају и користе.

У Европској унији основни правни оквир представља Општа уредба о заштити података – GDPR (Regulation (EU) 2016/679). Према члану 3, њена правила могу се примењивати и на компаније ван ЕУ које обрађују податке лица у ЕУ, под условима утврђеним Уредбом. Члан 5 утврђује основна начела обраде, међу којима су законитост, транспарентност, ограничење сврхе, минимизација података, ограничење чувања и поверљивост. За стриминг платформе посебно су значајни ограничење сврхе и минимизација података, јер подразумевају да се подаци прикупљају за конкретне сврхе и у обиму неопходном за њихово остваривање.

Члан 6 GDPR-а захтева постојање правног основа за обраду, као што су пристанак корисника, извршење уговора, законска обавеза или легитимни интерес. Према члановима 13 и 14, корисник мора бити информисан о сврси и правном основу обраде, врстама података, роковима чувања, примаоцима података и својим правима. GDPR корисницима даје и конкретна права, међу којима су право на приступ подацима (члан 15), исправку (члан 16), брисање (члан 17), ограничење обраде (члан 18) и преносивост података (члан 20).

Посебно је значајно профилисање. Члан 4 GDPR-а дефинише га као аутоматизовану обраду података ради процене личних аспеката појединца, укључујући његова интересовања, понашање и преференције. Код музичких платформи профилисање се може заснивати на подацима о слушаним песмама, претрагама, прескакању садржаја и дужини слушања, на основу чега алгоритми креирају персонализоване препоруке. Члан 22 додатно уређује право лица да не буде предмет одлуке засноване искључиво на аутоматизованој обради када она производи правне или слично значајне ефекте. Иако музичке препоруке обично немају такве последице, ова правила су значајна за разумевање односа између алгоритамске обраде и права корисника.

За глобалне платформе значајна су и правила о преносу података ван ЕУ. Чланови 44–49 GDPR-а прописују услове под којима се подаци могу преносити у треће државе, уз механизме као што су одлуке о адекватности и одговарајуће мере заштите, укључујући стандардне уговорне клаузуле.

У Сједињеним Америчким Државама не постоји јединствени савезни закон у потпуности упоредив са GDPR-ом, већ систем федералних и државних прописа. Посебно је значајан California Consumer Privacy Act (CCPA), измењен California Privacy Rights Act (CPRA). Овај оквир потрошачима даје, између осталог, права на приступ, брисање и исправку података, као и право да у одређеним ситуацијама одбију продају или дељење личних информација. CPRA је додатно ојачао контролу над осетљивим личним информацијама и њиховом обрадом.

У Републици Србији основни пропис је Закон о заштити података о личности („Службени гласник РС”, бр. 87/2018), који је у великој мери усклађен са европским концептом заштите података. Закон уређује начела обраде, права лица, обавезе руковалаца и обрађивача, пренос података у друге државе и надзор над применом закона. За кориснике дигиталних платформи значајна су права на приступ, исправку, брисање, ограничење обраде и преносивост података. Преносивост је уређена чланом 36, док Повереник врши надзор над применом закона.

Циљ правне заштите приватности, у контексту музичких стриминг платформи, није забрана обраде података, јер су одређени подаци неопходни за креирање налога, наплату, техничко функционисање и персонализацију услуге. Кључно је разликовати податке неопходне за пружање услуге од података који се користе за профилисање, оглашавање и аналитику. GDPR, CCPA/CPRA и српски закон разликују се по структури и обиму, али заједнички потврђују значај јасне сврхе обраде, правног основа, транспарентности и права лица на које се подаци односе.

За разлику од глобалног тржишта, за Србију није доступан исти обим јавно објављених индустријских података. *IFPI* у свом јавно доступном извештају не даје детаљну анализу српског тржишта упоредиву са највећим националним тржиштима. Због тога је код домаћег контекста неопходан опрез при коришћењу комерцијалних процена.

Statista Market Insights Србију обухвата у својој анализи дигиталне музике. Њихова дефиниција дигиталног музичког тржишта укључује музички стриминг, преузимање музике, огласно подржане сервисе и претплатничке сервисе на захтев, а база обухвата показатеље као што су приходи, број корисника, просечан приход по кориснику и стопа продора. Према истој методологији, стриминг представља највећи сегмент дигиталног музичког тржишта у Србији. То показује да се и домаће тржиште уклапа у ширу трансформацију музичке индустрије, иако се обим тржишта и потрошачке навике разликују од великих европских и светских тржишта.

За домаће ауторе дигиталне платформе представљају могућност да њихова музика буде доступна публици која није ограничена на Србију. То може бити посебно значајно за регионално тржиште, дијаспору и публику која прати одређене жанрове и извођаче независно од националних граница.

Истовремено, присуство на глобалној платформи не гарантује и видљивост. Огроман број доступних снимака значи да се домаћи садржаји такмиче за пажњу не само са регионалном већ и са светском продукцијом. Алгоритамске препоруке, листе и персонализовани прикази зато могу имати значајан утицај на то да ли ће корисник уопште доћи до одређеног домаћег извођача.

У овом контексту треба посматрати и питање података. Корисник у Србији који користи глобалну платформу истовремено је део глобалног система обраде података. Његове навике слушања могу се обрађивати у оквиру инфраструктуре која превазилази националне границе. Због тога су питања транспарентности, правног основа обраде, преноса података и права корисника релевантна и за домаће дигитално окружење.

МОГУЋА РЕШЕЊА И ПРЕПОРУКЕ

Заштита приватности корисника на стриминг платформама не значи потпуно одустајање од прикупљања и обраде података. Одређене информације неопходне су за функционисање сервиса, управљање корисничким налогом, наплату претплате, безбедност система и пружање појединих услуга. Питање приватности постаје сложеније онда када није јасно раздвојено који су подаци неопходни за пружање услуге, а који се прикупљају ради профилисања, оглашавања или детаљније анализе понашања корисника. У том погледу, принцип минимизације података подразумева да се прикупљање ограничи на информације које су потребне за унапред одређену и јасно дефинисану сврху.

Посебно је важно да корисник може да разуме шта се са његовим подацима дешава. Политика приватности не би требало да буде само формални документ који се прихвата приликом регистрације, већ средство помоћу којег корисник може да сазна које податке платформа прикупља, због чега их прикупља, колико дуго их задржава и са ким их може делити. У том смислу, значајно је јасно разликовати податке који су неопходни за коришћење услуге од оних који се користе за персонализацију, профилисање и оглашавање. Што је та разлика кориснику видљивија, то је већа и могућност да донесе информисану одлуку о коришћењу одређених функција платформе.

Контрола над персонализацијом представља још једно важно питање. Корисник би, када је то технички и правно могуће, требало да има могућност да ограничи одређене облике персонализације или профилисања и да једноставно приступи подешавањима која се односе на приватност. Тиме се однос између платформе и корисника не своди само на аутоматизовану обраду података. Кориснику се оставља одређени степен избора у погледу начина на који ће његови подаци бити коришћени, што је посебно значајно у систему у којем алгоритми имају све већу улогу у избору музичког садржаја.

Већ приликом развоја самог сервиса заштита приватности требало би да буде узета у обзир, а не тек након његовог успостављања. Управо на томе се заснива принцип „приватности по дизајну”, који подразумева укључивање заштите података у пројектовање алгоритама, система препорука и начина прикупљања и обраде података. То се односи и на податке који нису неопходни за основно функционисање услуге, чију употребу треба ограничити када за њу не постоји јасно оправдање. Додатни изазов представљају пренос и обрада података између различитих држава и правних система, због чега је неопходно обезбедити одговарајуће механизме њихове заштите и у таквим ситуацијама.

Одговорност за заштиту приватности, међутим, не може бити пребачена искључиво на корисника. Условима коришћења и политикама приватности често се приступа рутински, без детаљног читања и разумевања свих последица обраде података. Зато одговорност имају и саме платформе, пре свега кроз транспарентније представљање начина на који алгоритми функционишу, разумљивија објашњења о обради података и ефикасније механизме за остваривање права корисника. Минимизација података, транспарентност, већа контрола корисника и ограничење непотребног профилисања могу се посматрати као међусобно повезане мере које омогућавају да персонализација музичког искуства не буде остварена на рачун права на приватност.

ЗАКЉУЧАК

Дигитални медији значајно су променили музичку индустрију. Промене се не односе само на начин дистрибуције музике, већ и на пословне моделе, улогу посредника, начин откривања садржаја и однос између музичке индустрије и публике. Стриминг платформе један су од најзначајнијих резултата те трансформације и данас представљају основни начин приступа великом делу музичког садржаја. Њихова предност огледа се у доступности великог броја музичких садржаја, једноставности коришћења и могућности персонализације. Алгоритми на основу података о понашању корисника прилагођавају препоруке његовим интересовањима. Ипак, персонализовано искуство није могуће посматрати одвојено од прикупљања и обраде

података на којима се такве препоруке заснивају. Приватност је зато једно од важних питања функционисања савремених музичких платформи. Корисник није само слушалац музике већ и извор података који се користе за унапређивање услуге, креирање препорука, задржавање пажње и развој пословних модела. Подаци о навикама корисника на тај начин добијају и конкретну економску вредност, јер могу да се користе за персонализацију услуге, оглашавање и остваривање прихода. Управо због тога потребно је јасно разликовати податке који су неопходни за функционисање услуге од оних који се прикупљају у друге сврхе. Правни оквири, укључујући GDPR и Закон о заштити података о личности у Србији, постављају важне стандарде за заштиту права појединаца. Случајеви попут новчане казне изречене компанији Spotify показују да се ти стандарди примењују и у пракси. Ипак, правна регулатива сама по себи не решава све проблеме. Заштита приватности зависи и од начина на који платформе пројектују своје системе, од транспарентности алгоритама, техничке безбедности и могућности корисника да разумеју и контролишу употребу својих података. Развој вештачке интелигенције, сложенији системи препорука и све веће повезивање различитих дигиталних услуга вероватно ће додатно повећати количину и значај података који се обрађују. Заштита приватности због тога не би требало да буде посматрана као препрека технолошком развоју. Она би требало да буде укључена у сам процес развоја дигиталних услуга, од начина прикупљања података до њихове употребе и чувања. Будући развој музичких платформи зато ће, поред технолошких и пословних питања, све више зависити и од начина на који се успоставља однос између персонализације и права корисника. Кориснику је потребно омогућити квалитетно и прилагођено музичко искуство, али истовремено и јасне информације о томе који се подаци прикупљају, због чега се користе и у којој мери он може да утиче на њихову употребу. Такав приступ може допринети развоју дигиталних медија и музичке индустрије у којем технолошки напредак не искључује заштиту приватности, већ је подразумева.

РЕФЕРЕНЦЕ

Gervais, D. J. (2019). *The Future of Music: Competing Interests and Conflicting Values in the Digital Age*. Cheltenham: Edward Elgar Publishing.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven, CT: Yale University Press.

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119/1. europa.eu

IFPI. (2026). *Global music report 2026: State of the industry*. https://www.ifpi.org/wp-content/uploads/2026/03/GMR2026_SOTI.pdf

IFPI. (2026). Data & analysis: Methodology. In *Global music report 2026*. Приступљено 02.09.2026. <https://globalmusicreport.ifpi.org/>

Integritetsskyddsmyndigheten [IMY]. (2023). *Administrative fee against Spotify*. Приступљено 02.09.2026. <https://www.imy.se/en/news/administrative-fee-against-spotify/>

Morris, J. W. (2015). *Selling Digital Music, Formatting Culture*. University of California Press. Oakland, CA: University of California Press.

noyb – European Center for Digital Rights. (2023). *Spotify fined €5 million for GDPR violation* [Press release]. Приступљено 02.09.2026. <https://noyb.eu/en/spotify-fined-eu-5-million-gdpr-violation>

Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You*. New York, NY: Penguin Press. **Wikström, P. (2020).** *The Music Industry: Music in the Cloud*. Cambridge: Polity Press.

Повереник за информације од јавног значаја и заштиту података о личности. (н.д.). *Надлежност Повереника и заштита података о личности*. www.poverenik.rs

Закон о заштити података о личности. (2019). *Службени гласник РС*, бр. 87/2018.

Statista. (2026). *Digital music – Serbia* [Market insight]. Приступљено 31.08.2026. <https://www.statista.com>

Statista. (2026). *Music, radio & podcasts – Serbia* [Market insight]. Приступљено 31. 08. 2026. from <https://www.statista.com>

Toffler, A. (1980). *The Third Wave*. New York, NY: William Morrow and Company.

Hesmondhalgh, D. (2019). *The Cultural Industries*. London: Sage.

АЛГОРИТМИ У МЕДИЈИМА И ПРИВАТНОСТ ГРАЂАНА: АНАЛИЗА САВРЕМЕНИХ КИНЕСКИХ ИСТРАЖИВАЊА

Предраг Рава¹

Сажетак

Циљ овог рада јесте да, на основу анализе савремених кинеских истраживања, прикаже на који начин развој вештачке интелигенције мења однос између медија, алгоритама, приватности и медијске писмености. Полази се од претпоставке да се заштита приватности у ери вештачке интелигенције не може обезбедити искључиво законским регулативама, већ захтева интегрисани приступ који повезује комуникологију, етику, право, информатику и медијску писменост, који ће грађанима омогућити да критички разумеју начине на које ВИ системи прикупљају, обрађују и користе њихове податке. Рад нуди могуће одговоре на питања: како примена вештачке интелигенције мења професионалну праксу новинара и начин производње медијског садржаја; на који начин корисници доживљавају садржаје које производи вештачка интелигенција и како се развија поверење у алгоритмски генерисане информације; какве импликације развој ВИ има на заштиту приватности, безбедност података и медијску писменост грађана?

Кључне речи: вештачка интелигенција, алгоритми, медији, приватност, медијска писменост

¹ Удружење новинара Србије, Београд, Србија
e-mail: predrag.rava@gmail.com

УВОД

Развој генеративне вештачке интелигенције (AI – Artificial Intelligence), односно, алгоритмског препоручивања садржаја и аутоматизованог новинарства отворио је питања која превазилазе технолошку димензију и улазе у област људских права, приватности, професионалне етике и медијске писмености. Управо због тога питање приватности данас више није довољно посматрати искључиво кроз правни оквир заштите личних података. Оно подразумева разумевање начина на који алгоритми прикупљају, обрађују и користе информације о корисницима, како би персонализовали садржај, предвиђали понашање публике или унапредили рад ВИ система. Посебан изазов представља чињеница да се вештачка интелигенција све интензивније користи у новинарству. ВИ данас учествује у прикупљању података, писању вести, уређивању садржаја, персонализацији информација, препознавању трендова и модерацији коментара.

Аутоматизовано новинарство је већ након експерименталне фазе постало саставни део савремених медијских система, посебно у земљама које интензивно улажу у развој дигиталних медија, међу којима се Кина издваја као један од најзначајнијих примера. Код нас се често цитирају углавном англоамерички извори, док су кинеска емпиријска истраживања нажалост знатно мање заступљена.

Развој генеративне вештачке интелигенције повећава могућности персонализације медијских садржаја, али и обим прикупљања и обраде личних података, што приватност поставља у само средиште савремених комуникационих истраживања. Савремени ВИ системи, захваљујући способности симулирања реципрочне комуникације, стварају утисак интерперсоналне блискости, што додатно повећава спремност корисника да деле приватне податке, професионалне дилеме или емоционалне проблеме. Што је алгоритам успешнији у предвиђању корисничког понашања, то постаје зависнији од обраде личних података, па све више пажње привлаче питања његове транспарентности, одговорности за ВИ-генерисани садржај, заштите ауторских права, безбедности података и очувања приватности грађана.

ТЕОРИЈСКИ ОКВИР

У класичним моделима масовне комуникације новинар је био посредник између догађаја и публике. Развој генеративне вештачке интелигенције представља једну од највећих трансформација медијског система. Док су раније дигиталне технологије првенствено служиле као алати за дистрибуцију садржаја, савремени системи вештачке интелигенције учествују у писању новинских текстова, уређивању садржаја, персонализацији информација, превођењу, анализи великих скупова података, модерирању коментара и креирању мултимедијалних садржаја. Превазиђен је првобитни период аутоматског генерисања информација за финансијске извештаје, спортске вести или временску прогнозу. Истовремено, алгоритми одређују које ће информације бити видљиве појединим корисницима, којим редоследом ће бити представљене и на који начин ће бити интерпретиране. Тиме ВИ постаје један од најважнијих посредника између медија и публике.

Медији су имали ту срећу да се њихов развој од самог почетка преплиће са развојем савремених друштвених наука, као што су социологија и психологија, које су често истраживале нове облике комуникације. Већ саме почетке развоја електронских медија пратили су аутори који су припадали Франкфуртској школи. Био је то период настанка драгоцених теорија, али укупно гледано и фаза посматрања медија као једносмерних канала комуникација у којој је публика само пасивни посматрач. Тада је углавном истицана негативна, манипулативна улога медија као све доминантнијег агенса социјализације. Тако је Теодор Адорна сматрао да је култура постала роба и да масовни медији производе лаку забаву која пасивизира друштвену свест људи (Adorno, 1947/1989). У каснијим годинама уследио је период током ког публика није посматрана као пасивни реципијент који само опонаша медијски садржај.

Једну од најутицајнијих теорија за разумевање савремених медијских промена развио је Маршал Маклуан шездесетих година прошлог века. Његова позната тврдња да је „медиј порука“ (McLuhan, 1964) полази од претпоставке да структура – или природа медија кроз који се комуникација одвија снажније утиче на људе од самог садржаја који се њиме преноси. Маклуан је сматрао да сваки медиј „проширење чула“ и да се на тај начин мења начин на који људи опајају свет, организују друштвене односе, доносе одлуке и обликују сопствену стварност (видети Рава, 2015). Сматра да су и у прошлости технолошке промене утицале на целокупну структуру друштвене комуникације, а као пример наводи проналазак алфабета. Иако је својевремено називан технодетерминистом, данас смо сведоци да се његова „пророчанства“ обистинјују, посебно након развоја интернета у комерцијалне сврхе.

Начин представљања информације обликује њено значење и док су у класичним медијима оквир приче одређивали новинари и уредници, сада тај оквир све чешће обликују алгоритми који одлучују које ће чињенице бити истакнуте, које маргинализоване, а које потпуно изостављене из комуникационог процеса, те тако утичу и на начин на који публика разуме друштвену стварност. Парадокс савремених медија огледа се у томе што публика алгоритмаске одлуке често доживљава као неутралније управо зато што их доноси машина, иако они функционишу на основу података на којима су тренирани, критеријума и циљева које дефинишу медијске организације, које их користе.

Једну од новијих теорија о дигиталној економији развила је Шошана Зубоф у делу *The Age of Surveillance Capitalism* (Zuboff, 2019). Према њеном мишљењу, савремене дигиталне платформе не прикуљају податке искључиво ради унапређења услуга, већ их користе као основни економски ресурс за предвиђање и обликовање будућег понашања корисника. Дигитална економија тако све више почива на „капитализму надзора“, у којем људско искуство постаје сировина за предвиђање и обликовање будућег понашања корисника. У таквом окружењу границе између медија, технологије и тржишта постају све мање видљиве.

Са тим у вези, треба се присетити критичке перспективе Антонија Грамшија и његовог концепта културне хегемоније о ком је писао док је био у затвори 30-их година прошлог века. Иако је овај појам настао много пре развоја дигиталних технологија, он може бити изузетно користан за разумевање савремених алгоритамских система. Грамши је сматрао да се друштвена моћ најефикасније одржава онда када постане невидљива и када се постојећи поредак прихвата као природан. Тако се, кроз институције и свакодневне друштвене праксе, политичке и културне пристрасности могу репродуковати (видети Gramsci, 1951).

У дигиталном окружењу алгоритми могу допринети управо таквом облику „невидљиве моћи“. Њихове одлуке често се представљају као технички неутралне, иако у себи садрже вредносне претпоставке, економске интересе и политичке приоритете њихових креатора. У том значењу се данас може препознати нова врста доминације – алгоритмуска хегемонија у којој се кроз медије одређује које ће информације бити видљиве, коме ће бити приказане и на који начин ће бити интерпретирани.

Сваки клик, свака претрага, свако задржавање погледа на екрану и свака интеракција са ВИ системом производе нове информације које алгоритми анализирају. У таквом систему корисник више није само пасивна публика медија. Он постаје примарни извор података. Тиме се граница између комуникације и прикуљања података додатно замагљује. Данас се најчешће користе језички чет-ботови као што су: ChatGPT, DeepSeek, Gemini или Claude, са којима корисници често добровољно деле информације које раније нису били спремни да саопште ни претраживачима ни друштвеним мрежама. Кроз нови парасоцијални однос овај осећај реципрочности може повећати поверење корисника, али и њихову спремност да деле личне информације, професионалне дилеме или емоционална искуства.

У овом раду се предлаже коришћење новог појма – **симулирана реципрочна интерактивност**, којим се означава специфичан комуникациони однос у коме корисник има утисак да учествује у узајатној интерперсоналној комуникацији, иако друга страна нема свест, емоције нити стварну намеру. Овај феномен се директно надовезује на концепт симулакру² Жана Бодријара (Bodrijar, 1991), где копије и симулације преузимају улогу стварности. Тако концепт стар више од четири деценије, сада одевен у ново рухо представља још већи изазов за истраживаче.

Предмет овог рада јесте критичка анализа научних сазнања са циљем идентификовања кључних трендова, теоријских приступа и импликација за заштиту приватности и развој медијске писмености. Полазну основу чини анализа пет савремених кинеских истраживања објављених у периоду од 2023. до 2026. године. Избор ових радова није случајан, јер Кина данас предњачи у развоју генеративне вештачке интелигенције и њеној примени у медијима. Нажалост, кинески аутори се ретко преводе на српски језик, иако они користе различите методолошке приступе што омогућава сагледавање феномена из више углова. То омогућава да се резултати истраживања не посматрају изоловано, већ као елементи јединственог процеса трансформације савременог медијског система. Поред квалитативних интервјуа и анкетних истраживања они користе и експерименталне неурофизиолошке методе које су за наше услове веома скупе, па би резултати и закључци њихових истраживања могли бити од велике користи за проучавање српског медијског екосистема.

ВИ МЕДИЈИ И ПОВЕРЕЊЕ ЈАВНОСТИ

Досадашња истраживања најчешће су била усмерена на питање да ли су алгоритми способни да производе квалитетне новинарске садржаје. Наспрам тога, Јан Ли је у раду „The impact of automated journalism on media bias, accuracy, and public trust: Evidence from young Chinese news consumers” (Li, 2026), испитао како изложеност вестима које генерише вештачка интелигенција утиче на перцепцију пристрасности, тачности и поверења код младих, дигитално компетентних корисника вести у Кини. На тај начин у средишту интересовања је перцепција публике, а не само техничке могућности ВИ система.

Циљ је био да се на узорку од 467 младих кинеских корисника вести старости између 18 и 35 година, утврди како изложеност ВИ-генерисаним вестима утиче на перцепцију медијске пристрасности, поверење у медије и процену тачности аутоматизованог новинарства. Студија је имала три међусобно повезана циља. Прво, да се утврди у којој мери повећана изложеност

² Симулакрум, према Бодријару представља сложен концепт, али који уопштено може да се дефинише као копија која нема свој оригинал. У питању је хиперреалност која уз помоћ слика, знакова или медија и друштвених мрежа симулира стварност, па тако створена илузија делује реалније од саме стварности.

садржају који генерише AI утиче на перцепцију медијске пристрасности. Други циљ јесте да се испита да ли постоји повезаност између поверења у аутоматизовано новинарство и перцепције тачности генерисаних вести. Трећи циљ је да се испита како политичка опредељеност утиче на поверење у ВИ-садржај.

Резултати су показали да чешћа изложеност вестима које производи вештачка интелигенција доводи до мање перцепције медијске пристрасности, већег поверења у ВИ садржаје и више процене њихове тачности (Li, 2026). Овакав налаз представља важан теоријски допринос савременим медијским студијама. Посебно су били у фокусу млади, јер представљају генерацију „дигиталних урођеника” која вести углавном прати преко алгоритмски прилагођених садржаја на интернету. То се донекле може приписати технолошкој навикнутости корисника. Закључак је и да публика не мора нужно познавати начин рада алгоритама да би их доживела као објективније од људских новинара. Напротив, управо сложеност и технолошка природа ВИ система, посебно брзина обраде података, могу створити утисак непристрасности код публике, чак и када такви садржаји немају истраживачку дубину или сложену анализу.

Алгоритам се често перципира као нешто што је ослобођено политичких ставова, емоција или идеолошких интереса који се традиционално повезују са људским ауторима. Међутим, утврђено је да управо политичка оријентација значајно детерминише поверење у аутоматизоване медијске садржаје, па се упозорава на то да вештачка интелигенција може репродуковати и појачавати постојеће пристрасности, нарочито у социо-културним областима.

Ово истраживање заснивало се на четири теоријска приступа. Први приступ је **Теорија употребе и задовољења потреба** (*Uses and Gratifications Theory* – UGT) која полази од претпоставке да публика није пасивна, већ активно бира медије који најбоље задовољавају њене потребе. Други приступ чини **Теорија вратарења** (*Gatekeeping*), како би се анализирала могућност да алгоритми уместо људи буду „чуvari капије”. Трећи приступ је **Теорија уоквиравања** (*Framing Theory*), према којој начин техничког представљања информације снажно утиче на њено тумачење. Четврти приступ се ослања на **Моделе медијског поверења** (*Media Trust Models*) које су развили Матијас Коринг и Јорг Матес (Kohring & Matthes, 2007), према којима поверење у медије настаје кроз дуготрајно искуство са тачношћу, поузданошћу и транспарентношћу. Ако корисници више пута добијају информације које сматрају тачним и неутралним, расте њихово поверење у ВИ систем. Наравно, личне карактеристике, склоности и политичка опредељеност корисника су детерминанте које не треба занемарити.

Овај налаз отвара важно питање за будућа истраживања: да ли публика ВИ садржаје сматра објективнијим зато што заиста препознаје њихову неутралност или зато што претпостављује да машина нема политичке и идеолошке интересе које има човек? Другим речима, могуће је да се перцепција непристрасности заснива више на веровању у технолошку неутралност него на стварној процени квалитета садржаја.

На основу налаза, ауторка овог истраживања предлаже увођење транспарентних система контроле ВИ алата. Једна од могућности јесте формирање посебних комисија које би надзирале рад алгоритама, проверавале податке коришћене за тренирање система и оцењивале квалитет произведеног садржаја. Такве комисије могле би да окупе стручњаке за вештачку интелигенцију, новинаре и етичаре, са задатком да идентификују потенцијалне пристрасности, предлажу корекције и редовно обавештавају јавност о раду ВИ система. Такође се предлаже веће укључивање публике. На пример, корисницима би могла бити пружена могућност да бирају да ли желе да читају: потпуно аутоматизоване вести, ВИ генерисане вести уз људску редакцију, или садржаје које су написали људи. Поред тога, медијске платформе требало би јасније да објашњавају како алгоритми бирају и рангирају вести како би корисници били свесни могућих ограничења и пристрасности.

НЕУРОКОГНИТИВНИ АСПЕКТИ ПОВЕРЕЊА: ШТА МОЗАК ГОВОРИ О ВИ САДРЖАЈИМА?

Док је Ли (Li, 2026) анализирала свесне ставове и процене корисника AI садржаја, истраживање које потписују Чен Гонг и сарадници приступа истом проблему из потпуно другачије перспективе – кроз неурофизиолошка мерења активности мозга. Њихово истраживање под називом „AI voices reduce cognitive activity? A psychophysiological study of the media effect of AI and human newscasts in Chinese journalism” (Gong, 2023), мери начин на који мозак обрађује информације.

Аутори су користили електроенцефалографију (EEG) и ERP (*event-related potentials*) како би испитали да ли људи различито обрађују информације које читају или слушају када верују да их је произвео човек или вештачка интелигенција. За разлику од анкетних истраживања, EEG омогућава регистровање мождане активности током саме обраде информација, пружајући увид у когнитивне процесе који нису доступни путем самопроцене испитаника. Циљ рада био је да испита психофизиолошке ефекте медија. Треба напоменути да је и пре појаве ВИ у масовној комуникацији, већ 2004. године предлагано је коришћење психофизиолошких метода за истраживање ефеката медија. Иако 2006. године вештачка интелигенција још није постојала у данашњем облику, истраживачи су проучавали штампане и онлајн новине користећи моделе праћења очију (*eye-tracking*). Гонг као пример наводи да Бучера и Шумахера (Bucher & Schumacher, 2006) који су испитивали како тип медија утиче на пажњу и селективност публике.

Ово истраживање је испитало разлике у когнитивним и неурофизиолошким реакцијама слушалаца на вести које чита људски глас у поређењу са ВИ генерисаним гласом, уз додатно раздвајање на емотивни и неутрални садржај. Студија је обухватила укупно 30 испитаника, углавном млађих одраслих особа узраста између 18 и 40 година, међу којима је било 16 жена и 14 мушкараца. Сви испитаници су били десноруки, имали нормалан слух и вид, нису претрпели повреду главе у недељи која је претходила експерименту, нити су узимали психостимулативне или друге лекове који утичу на централни нервни систем. Такође, ни они ни чланови њихових породица нису имали историју психијатријских или неуролошких поремећаја, нити сродних стања (нпр. епилепсију).

На EEG сигнал значајно утичу очни покрети, трептање, мишићна активност, срчана активност и електрични шум, што представља озбиљан проблем у анализи и интерпретацији EEG података. Због тога су ручно уклањани артефакти изазвани трептањем, покретима очију и покретима главе у специфичним експерименталним условима. Резултати показују да људски глас изазива снажније неурокогнитивне реакције од ВИ генерисаног гласа. Посебно су значајне разлике у **бета таласима** у левој задњој темпоралној регији, што указује на то да је мозак учесника боље обрађивао, разумевао аудитивне информације и ефикасније их складиштио у радној меморији када су слушали људски у поређењу са ВИ гласом.

Будући да тренутно синтетизовани гласови у постојећим технологијама вештачке интелигенције још увек не могу ефикасно да обраде специфичне случајеве акценатског ритма, алитерације и изговора у кинеском језику, људски гласови могу показивати израженије промене у обради слогова и акцената у поређењу са синтетизованим гласовима. На тај начин они изражавају више емоција и сигналних елемената и изазивају снажније когнитивно-емоционалне реакције код слушалаца, што се у овој студији пре свега огледа кроз активност можданих таласа.

Људска комуникација задржава одређене психолошке предности које алгоритми још увек не могу у потпуности репродуковати. Синтетички глас слабије преноси парангливистичке сигнале као што су интонација, паузе и ритам, што смањује когнитивну обраду и пажњу корисника. Поред тога, ERP резултати и интеракциони ефекти емоционалног садржаја и врсте гласа показали су да људски глас изазива јачи когнитивни ефекат, што може одражавати веће поверење учесника у кредибилитет и тачност људског новинарског гласа. Утврђено је да што је веће коришћење друштвених мрежа, то је већа и процена кредибилитета генерисаних вести.

У раду се наводи да емоционални садржај који емитује AI глас такође може изазвати ефекат „језиве долине” (*uncanny valley*)³. У питању је феномен о ком је у кратком есеју још 1970. године писао Машахиро Мори, а који је јавности познатији након превода из 2012. године (Mori, 2012). Нека истраживања повезују ВИ новинарство са проблемом лажних вести. Гонг помиње и ауторе Пеникука и Ранда који сматрају да су људи склони да верују дезинформацијама због менталних пречица (хеуристика). Исти аутори указују да употреба ВИ у великим медијима (нпр. *New York Times*) може чак смањити перцепцију кредибилитета самог извора.

На први поглед, налази које је добио Гонг делују супротно резултатима истраживања које је представила Ли, у ком се показује да млади Кинези вести произведене вештачком интелигенцијом често сматрају објективнијим и мање пристрасним. Алгоритам се често доживљава као непристрасан управо зато што није човек, а заправо иза сваког AI система налазе се људи који одређују циљеве модела, бирају податке за тренирање, дефинишу правила филтрирања садржаја и обликују алгоритамске одлуке. Међутим, ова два истраживања заправо испитују различите нивое људског искуства. Док је прво истраживање показало да млади Кинези ВИ вести често доживљавају као мање пристрасне и тачније од традиционалних медијских садржаја, ово друго је показало да људи когнитивно снажније реагују на људски глас него на ВИ глас.

Другим речима, једно истраживање говори о свесним ставовима и перцепцијама публике према новинарству, док друго говори о подсвесном начину на који људски мозак обрађује саму вест. Та два налаза нису нужно у супротности, већ могу да укажу на занимљиву појаву према којој људи могу више да верују алгоритмски произведеном садржају, али у исто време и даље емоционално и когнитивно снажније реагују на директну људску комуникацију, јер их људски новинар више ангажује на когнитивном нивоу. Управо зато највећи изазов савременог медијског система можда није сам развој вештачке интелигенције, већ развој критичког разумевања начина на који она функционише.

³ Ефекат „језиве долине” (*uncanny valley*) се јавља када недовољно природни, антропоморфни прикази изазивају подсвесну нелагодност и одбацавање код публике. Када је антропоморфизација висока и технички беспрекорна, публика лакше формира емоционалну везу и поверење, док је при ниској или вештачкој антропоморфизацији формирање емоционалног поверења готово немогуће. Ипак, овај однос није потпуно линеаран, јер када копија човека постане готово савршена, али уз ситне недостатке, код посматрача се ствара осећај језе и нелагодности.

УСВАЈАЊЕ ВИ НОВИНАРСТВА ИЗ ПЕРСПЕКТИВЕ НОВИНАРА

Хао Сјанг Луо је у раду „Factors influencing the adoption of generative AI technology by Chinese mainstream media journalists: A field study based on J Province broadcasting and television”, спровео још једно драгоцено истраживање у овој области испитујући ставове новинара телевизијске мреже у кинеској провинцији Ђангси (Luo, 2024). У периоду од септембра 2023. до јануара 2024. године, користећи комбинацију партиципативног посматрања и дубинских интервјуа са тридесет новинара, анализирани су фактори који утичу на усвајање генеративне вештачке интелигенције у свакодневном раду редакција. Иако већина истраживања користи квантитативне методе (упитнике и моделовање структуралних једначина), ова студија наглашава значај квалитативних метода, као што су посматрање и дубински интервјуи. Узете су у обзир и варијабле као што су старост, пол, искуство.

На основу теоријског оквира, формулисана су следећа истраживачка питања:

1. Какво је тренутно стање усвајања генеративне ВИ технологије међу новинарима мејн-стрим медија?
2. Који фактори подстичу почетно и континуирано усвајање ВИ технологије?
3. Које су кључне препреке у усвајању генеративне ВИ технологије међу новинарима?

Укратко, циљ је био испитати шта медијски радници мисле о томе како вештачка интелигенција мења обрасце интеракције човек–машина и како то утиче на професионални идентитет новинара.

Као теоријску основу користио је Обједињену теорију прихватања технологије (UTAUT) и ТОЕ оквир (*Technology–Organization–Environment*), чиме је повезао индивидуалне ставове запослених са организационим условима рада.

UTAUT модел дефинише четири кључна фактора усвајања технологије:

- *Очекивани учинак* – веровање да технологија побољшава радне перформансе;
- *Очекивани напор* – лакоћа коришћења саме технологије;
- *Социјални утицај* – утицај колега и средине на одлуку о коришћењу;
- *Олакшавајући услови* – организациона и техничка подршка унутар куће.

ТОЕ оквир анализира усвајање технологије кроз три велике димензије: технологију, организацију и окружење. Он омогућава разумевање фактора као што су организациона култура, расподела ресурса, политичке и тржишне околности, као и конкурентски притисак са којим се медији суочавају. Посебно је значајно што се питање приватности у овом истраживању не односи искључиво на крајње кориснике медија, већ и на саме медијске раднике.

Резултати показују да почетно интересовање новинара за ВИ произлази првенствено из радозналости и друштвеног утицаја. Појава великих језичких модела крајем 2022. године изазвала је велико интересовање запослених у медијима, али је код већине испитаника оно убрзо опало. Само мањи број новинара наставио је редовну употребу AI алата, углавном за рутинске задатке попут сажимања текстова, претраге информација или припреме нацрта садржаја. Много значајнији од самог нивоа коришћења јесу разлози због којих новинари

показују резерву према AI системима. Испитаници наводе међусобно повезане проблеме као што су: ограничена поузданост генерисаних информација, могућност појаве чињеничних грешака, нејасно решена питања ауторских права, неправедна расподела користи од примене технологије, као и забринутост за информациону безбедност и заштиту података. Брине их то што употреба генеративне ВИ подразумева и уношење радних материјала, текстова, интерних докумената, фотографија и других података, што отвара питање контроле над информацијама које напуштају редакцију. У поређењу са новинарима, менаџмент је показивао мање изражен отпор. На послетку, допринос овог истраживања је и у томе што скреће пажњу на то да заштита приватности постаје саставни део професионалне етике и информационе безбедности медијских организација.

О ВЕШТАЧКОЈ ИНТЕЛИГЕНЦИЈИ У КИНЕСКИМ МЕДИЈСКИМ КУЋАМА: ПРИЈАТЕЉ ИЛИ НЕПРИЈАТЕЉ?

Дубински метод је коришћен и у студији под називом „Friend or foe? Human journalists’ perspectives on artificial intelligence in Chinese media outlets”, аутора Јанг Јуа и Кјуо Хуанга (Yu & Huang, 2021). Испитана је перцепције медијских практичара који раде у кинеској медијској индустрији о утицају вештачке интелигенције на запошљавање у медијима. У раду су формулисана два кључна истраживачка питања:

1. Како људски новинари који раде у кинеској медијској индустрији разумеју утицај AI технологије на њихове могућности запошљавања?
2. Како кинеске медијске организације комуницирају са новинарима о усвајању вештачке интелигенције, посматрано из перспективе самих новинара?

Да би се разумео контекст овог истраживања, неопходно је осврнути се на брзу технолошку еволуцију водећих кинеских медија. У децембру 2017. године кинеска државна новинска агенција Синхуа лансирала је своју напредну платформу за вештачку интелигенцију под називом *Media Brain*. Већ у марту 2018. године, ова агенција је премијерно представила први медијски садржај генерисан искључиво од стране машина. То су били видео-извештаји током два најважнија политичка заседања у земљи – Свекинеског народног конгреса и Кинеске народне политичке консултативне конференције. Платформи *Media Brain* било је потребно свега 15 секунди да аутоматски произведе и објави комплетну вест.

Поред тога, у сарадњи са кинеским интернет претраживачем Sogou.com, агенција Синхуа је развила првог AI водитеља вести на свету који је способан да ради 24 сата дневно и емитује вести на званичном сајту и друштвеним мрежама. Током маја 2020. године, ова сарадња је унапређена представљањем прве 3D верзије ВИ водитеља вести која је визуелно и акустички потпуно имитирала изглед и глас стварне новинарке (Jiang, 2020). Овај 3D виртуелни водитељ се без напора кретао по виртуелном студију, мењао фризуру и одећу како би се прилагодио контексту вести, а пројектован је са циљем да у будућности може самостално да „напусти” студио и извештава директно са терена.

Аутори Ју и Хуанг (Yu & Huang, 2021) напомињу да интеграција нових технологија у новинарску праксу није потпуно нови феномен у историји комуникација. Још 2009. године Универзитет Нортвестерн у Сједињеним Америчким Државама покренуо је систем *Stats Monkey* за аутоматско генерисање спортских извештаја. Од тада, аутоматизовано новинарство је почело да покрива финансије, спорт, временску прогнозу и практично све области за које су доступни јасно структурирани емпиријски подаци. До 2018. године, отприлике једна четвртина укупног садржаја агенције *Bloomberg News* у различитој мери се ослањала на аутоматизацију. Ипак, традиционалне новинске редакције су глобално биле релативно споре у прихватању ове врсте аутоматизације у поређењу са другим гранама, као што је, на пример, индустрија интелигентних видео-игара.

У настојању да се објасни овај феномен, у раду се истиче да би за разумевање савремених процеса од велике користи могла бити класична **Теорија дифузије иновација Еверета Роџерса**, која у друштвеним наукама има дугу историју емпиријских и концептуалних истраживања. Одлуке људи о томе да ли ће усвојити неку технолошку иновацију и колико дуго тај процес транзиције траје биле су у фокусу проучавања бројних научних дисциплина. Ова теорија је започела са класичним моделом дифузије, који испитује процесе ширења иновација међу члановима друштвеног система током времена путем специфичних комуникационих канала. Прихватање и усвајање неког производа, идеје или технологије никада се не дешава изоловано. Појединци и медијске организације показују различите нивое склоности ка ранијем или каснијем усвајању иновација у односу на остатак заједнице.

Савременији социолошки приступи теорији иновација додатно тврде да је свака технологија заправо производ који настаје у оквиру специфичне политичке, друштвене, економске и културне климе, те да је њено коначно усвајање дубински обликовано активним људским деловањем. Због тога је немогуће разумети саму технологију без темељног разумевања ширег друштвеног контекста у којем она оперише.

У овом емпиријском истраживању изабрано је укупно 18 новинара. Приликом узорковања пажљиво су узети у обзир тип медија, професионална позиција и дужина радног стажа, како би у узорку били равноправно заступљени различити типови кинеских медијских организација и улога. Дужина радног искуства испитаника у медијима кретала се у распону од 2 до 34 године. Њихове професионалне позиције биле су изразито разнолике и обухватале су: ТВ водитеље, репортере, уреднике рубрика, продуценте, лекторе, уреднике за друштвене мреже, водитеље ток-шоу програма, директоре за дигиталне медије, коментаторе и иностране дописнике. Изабране медијске куће обухватале су државне медије, комерцијалне медије и организације са мешовитим власништвом, са етаблираном репутацијом у континенталној Кини у оквиру радија, телевизије, штампе и друштвених мрежа. Полуструктурирани интервју садржао је 23 питања која су обухватала досадашње радно искуство новинара, њихова конкретна искуства у раду са вештачком интелигенцијом, као и хипотетичка питања о њиховим предлозима и визијама за будуће коришћење ВИ алата у радном окружењу.

Из квалитативне анализе података произашле су три главне теме. Добијени материјал указује на то да медијски практичари сматрају да ВИ суштински мења медијски пејзаж кроз оптимизацију структуре радне снаге и „ослобађање” људских новинара од репетитивних, рутинских послова. Такође, подаци показују да људски новинари испољавају високу прилагодљивост и професионалну отпорност, док саме медијске институције промовишу позитиван организациони наратив кроз интерне демонстрације нових ВИ технологија, тежећи ка остваривању већег утицаја на медијском тржишту. Добијени наводи јасно приказују икако учесници разумеју улогу ВИ у специфичним извештавањима током ванредних и кризних ситуација, као што је била глобална пандемија вируса COVID-19:

Резултати истраживања недвосмислено показују да новинари истовремено доживљавају вештачку интелигенцију и као фактор велике трансформације и као супериоран алат подршке. Они сматрају да је у питању технолошка иновација која може успешно да оптимизује радне процесе, замени рутинске послове и подигне ниво ефикасности, али не може у потпуности да замени саму суштину новинарске професије. Људски рад остаје кључан и незаменљив у доменима који захтевају креативност, интерпретацију контекста, емпатију и комплексно етичко одлучивање. Како би се обезбедио адекватан и одговоран уреднички надзор, нове технолошке иновације морају бити дизајниране тако да у сваком тренутку омогућавају људским уредницима пуну контролу над финалним медијским производом.

ИСТРАЖИВАЊЕ О ПРИМЕНИ ВИРТУЕЛНИХ ВОДИТЕЉА ЗАСНОВАНИХ НА ГЕНЕРАТИВНОЈ ВЕШТАЧКОЈ ИНТЕЛИГЕНЦИЈИ У ИЗВЕШТАВАЊУ

Наредно истраживање „Research on the application of generative AI-based virtual anchors in news reporting”, чији је аутор Мингјанг Ху (Hu, 2025), такође је драгоцено јер је било усредсређено на фундаментално питање: Могу ли виртуелни водитељи, оснажени савременим технологијама, да испуне друштвене улоге које се традиционално повезују са новинарством и медијским комуницирањем?

Кроз прикупљање анкетних упитника и примену методе анализе садржаја, Ху је систематски испитао тренутно стање примене виртуелних водитеља у новинарском извештавању, ниво прихватања од стране публике и њихов утицај на екосистем медијског комуницирања. Како би се одговорило на то питање, истраживање разматра три питања:

1. Да ли постоје разлике у прихватању виртуелних водитеља међу публиком различитих демографских карактеристика?
2. Какав је однос између врсте новинарског садржаја и кредибилитета који публика приписује виртуелним водитељима?
3. Какав структурни утицај масовна примена виртуелних водитеља има на целокупни екосистем новинарског комуницирања?

Због тога ова студија користи комплементаран научни приступ, интегришући теорије као што су: медијска екологија, теорија употребе и задовољења потреба и концепт миметичког окружења (мимеза-опонашање), како би систематски истражила механизме примене виртуелних водитеља у новинарском извештавању и њихов утицај на комуникациони екосистем.

Студија је изабрала репрезентативне емисије виртуелних водитеља са водећих платформи као што су *Xinhua News Agency*, *CCTV News*, *Bilibili* и *Douyin*, обухватајући пет категорија вести из области политике, финансија, друштва, животних стилова (*lifestyle*) и забаве. Упитник је дистрибуиран онлајн преко WeChat платформе („QuestionStar”) у периоду од 28. априла до 12. маја 2025. године. Методом стратификованог узорковања прикупљено је укупно 260 валидних упитника, при чему демографску структуру узорка чине 162 жене и 98 мушкараца (што комплетира укупан број испитаника).

Старосна структура узорка је следећа:

- 18–24 године: 69 испитаника (26,5%)
- 25–34 године: 56 испитаника (21,5%)
- 35–44 године: 56 испитаника (21,5%)
- 45 и више година: 75 испитаника (28,8%)

Анализа образовног нивоа указује на позитивну корелацију између образовног постигнућа и прихватања технологије, при чему високообразоване групе показују знатно већу отвореност према технолошким иновацијама. У погледу образовања, доминантну групу чине испитаници са универзитетским нивоом (40,4%). Утицај демографских карактеристика на прихватање виртуелних водитеља показује јасне групне обрасце. Старосна доб показала је најизраженији диференцирајући ефекат: скор прихватања у групи од 18 до 34 године био је значајно виши него у групи старијој од 35 година. Родне разлике, иако релативно умерене, остале су статистички значајне. Женски испитаници су показали нешто виши скор прихватања у односу на мушке испитаника.

Такође, уочен је јасан однос између учесталости конзумације вести и прихватања виртуелних водитеља. Високофреквентни корисници, који приступају вестима више пута дневно, показали су највиши ниво отворености. Фактори занимања такође индукују значајне групне ефекте: студенти и запослени у приватним компанијама имају знатно виши ниво прихватања него државни службеници, запослени у јавним институцијама и фриленсери.

Резултати недвосмислено показују да виртуелни водитељи уживају знатно већи степен прихваћености у вестима из области свакодневног живота, услужних информација и забаве (*lifestyle*) него у политичким вестима и вестима о ванредним и кризним догађајима. Публика углавном задржава резерву према њиховим способностима процене, дубинског тумачења и доношења судова.

ОД МЕДИЈСКЕ КА АЛГОРИТАМСКОЈ ПИСМЕНОСТИ – УМЕСТО ЗАКЉУЧКА

Иако се овај рад у највећој мери ослања на анализу савремених кинеских истраживања, његова основна запажања имају глобални значај. Брз развој генеративне вештачке интелигенције представља глобални процес који захтева интердисциплинарни приступ и нова емпиријска истраживања у различитим друштвеним и медијским системима, укључујући и Србију. Налази изнети у овом раду могу се јасно пројектовати и на домаћу медијску сцену. На пример, резултати истраживања „Вештачка интелигенција у медијима у Србији 2025.“, које је спровео **Центар за професионализацију медија и медијску писменост** (CEPROM, 2025), показују готово идентичан тренд као и кинеска емпиријска пракса: чак 92,8% домаћих новинара и уредника сматра да ВИ не може у потпуности и на професионалан начин да замени човека. Баш као и у светским оквирима, главна порука српских медијских професионалаца јесте да ВИ у новинарству представља корисног асистента у рутинским пословима, а не апсолутну замену за све сегменте новинарске професије.

Наравно, пенетрација вештачке интелигенције неће се одвијати истом брзином у свим медијима. Постоји разлика између великих, финансијски снажних медија који могу да приуште

такве иновације и мањих медија који се, пре свега, прибојавају замене, односно губитка досадашњих радних места. Последица таквог стања је могуће продубљивање неједнакости у медијској индустрији. Развој и примена иновација је и раније са собом доносила одређене ризике, али и нове могућности. Главна порука је да ВИ у новинарству не мора да доведе до замене новинара, већ до реструктурирања медијског рада, што може да буде надградња људске улоге која се тако помера ка креативности и етичкој процени.

Традиционални концепт медијске писмености, који је подразумевао способност грађана да дешифрују поруку, критички је анализирају и одговорно користе, постаје недовољан у ери алгоритмског управљања садржајем. Корисник медијског садржаја требало би, као и раније, да разуме значење информације, али сада мора бити способан да разуме и процесе њеног технолошког генерисања. Медијска писменост тиме прераста у **алгоритмску писменост**, која обухвата разумевање начина тренирања ВИ модела, извора података, препознавања алгоритмске пристрасности, као и механизма за персонализацију садржаја и рударење личних података.

Будући да генеративни системи симулирају реципрочну комуникацију, они код корисника стварају лажни осећај узајамног поверења. Кроз овај парасоцијални однос, грађани често добровољно деле интимне податке којима се ВИ модели непрекидно „хране”. Због тога питање приватности прераста оквира класичне информатичке безбедности и претвара се у проблем системске експлоатације и комерцијализације личних информација без експлицитног пристанка корисника. Стога се може закључити да се алгоритмска писменост појављује као критичка вештина препознавања дезинформација створених генеричким путем и проналажења корисних садржаја у медијском систему.

На основу теоријских и емпиријских налаза анализираних у раду, могу се дефинисати следеће практичне препоруке:

- **За медијске организације:** Увести обавезу јасног и транспарентног означавања ВИ-генерисаног садржаја универзалним симболима; креирати интерне етичке кодексе и јавно објавити политике о границама употребе аутоматизованих алата у редакцијама.
- **За новинаре и медијске раднике:** Развијати континуиране програме едукације који обухватају техничко управљање ВИ алатима, али и напредну обуку у области заштите сигурности извора и приватности података у дигиталном окружењу.
- **За образовне институције:** Интегрисати алгоритмску писменост у званичне курикулуме основног, средњег и високог образовања; учити ученике како функционишу велики језички модели и развијати код њих критичко промишљање алгоритмског доношења одлука.
- **За законодавце и регулаторна тела:** Унапредити постојећи правни оквир у области јавног информисања кроз стриктне одредбе о транспарентности алгоритама; законски обавезати платформе на јасно мапирање аутоматизованог садржаја и ускладити стандарде заштите података о личности са изазовима које доноси генеративна вештачка интелигенција.

На послетку, потребно је нагласити да, са обзиром на то коликом брзином се вештачка интелигенција развија и колико се њена примењивост мултипликује у медијима, постоји вероватноћа да су већ током писања овог рада добијена нова истраживачка сазнања која могу да оповргну или надграде све оно што смо до сада знали.

РЕФЕРЕНЦЕ

- Adorno, T. (1947/1989). *Dijalektika prosvjetiteljstva*. Sarajevo: Svjetlost, biblioteka Logos.
- Bodrijar, Ž. (1981/1991). *Simulacija i simulakrumi*. Novi Sad: Svetovi.
- Gong, C. (2023). „AI voices reduce cognitive activity? A psychophysiological study of the media effect of AI and human newscasts in Chinese journalism”. *Frontiers in Psychology*, 14.
- Gramsci, A. (1951). *Pisma iz zatvora*. Zagreb: Zora, Državno izdavačko preduzeće Hrvatske.
- Zuboff, S. (2019). *The age of surveillance capitalism*. Public Affairs.
- Yin, X. (2020). „Reconstruction of host's professional image from the perspective of intelligent media-Based on the appearance of "AI synthesis anchor" of Xinhua News Agency”. *The First China Xijing Intelligent Media Forum (CXIMF 2020)*.
- Yu, Y., & Huang, K. (2021). „Friend or foe? Human journalists' perspectives on artificial intelligence in Chinese media outlets”. *Chinese Journal of Communication*, 14(4), 409–429. doi.org
- Li, Y. (2026). „The impact of automated journalism on media bias, accuracy, and public trust: Evidence from young Chinese news consumers”. *Humanities and Social Sciences Communications*, 13, 688.
- Luo, H. (2024). „Factors influencing the adoption of generative AI technology by Chinese mainstream media journalists: A field study based on J Province broadcasting and television”. *Eurasia Journal of Science and Technology*, 6(6), 37–43.
- McLuhan, M. (1964). *Understanding media: The extensions of man*. McGraw-Hill.
- Mori, M. (2012). „The uncanny valley”. *IEEE Robotics and Automation Magazine*, 19(2), 98-100. (Original work „Bukimi no tani” published 1970 in *Energi*, 7(4), 33-35.).
- Rava, P. (2015). „Uticaj nasilja u filmu na ljudsko ponašanje”. *Kultura Polisa*: 12 (27): 313-329.
- CEPROM. (2025). „Veštačka inteligencija u medijima u Srbiji 2025: Koristan asistent, a ne zamena za novinare”. *Centar za profesionalizaciju medija i medijsku pismenost*. Pristupljeno 4. avgusta 2026. sa ceprom.rs.
- Hu, M. (2025). „Research on the application of generative AI-based virtual anchors in news reporting”. *Communications in Humanities Research*, 86(1), 114–122.

ПРЕТПОСТАВКА НЕВИНОСТИ У ДИГИТАЛНИМ МЕДИЈИМА У СРБИЈИ: АНАЛИЗА НАСЛОВА И ЛИДА НА ПОРТАЛИМА

Сандра Д. Иршевић¹

Сажетак

У раду се истражује начин на који се у рубрици црне хронике у онлајн медијима у Србији нарушава начело претпоставке невиности. Истраживање је усмерено на анализу наслова и лидова вести објављених у периоду од јануара до јуна 2026. године. Основна теза рада полази од претпоставке да дигитални медији у Србији, у настојању да привуку пажњу публике сензационалистичким садржајима, често прерано представљају осумњичена лица као учиниоце кривичних дела, чиме непосредно крше начело претпоставке невиности. Истраживање је засновано на квалитативној анализи одабраних објава домаћих онлајн портала, као и на нормативној анализи релевантног правног оквира. Посебна пажња посвећена је члану 73 Закона о јавном информисању и медијима, уз уважавање професионалних и етичких стандарда новинарске професије. Циљ рада је да идентификује најчешће облике кршења начела претпоставке невиности, као и да покаже на који начин поједине језичке конструкције и наративни обрасци у онлајн новинарству доприносе његовом нарушавању. Резултати истраживања указују да су сензационалистички формулисани наслови, недовољно опрезно и некритичко преношење информација које потичу од полиције и тужилаштва, као и изостављање јасних правних ограда, кључни механизми нарушавања претпоставке невиности. У закључку се истиче да је за промену постојеће медијске праксе неопходно доследније поштовање законских и етичких стандарда, али и континуирано професионално усавршавање новинара и уредника, будући да без развијене свести о одговорности јавне речи ни најквалитетнији нормативни оквир не може обезбедити потпуну заштиту начела претпоставке невиности.

Кључне речи: претпоставка невиности, дигитални медији, портали, хроника, приватност, медијска етика

¹ Сандра Д. Иршевић, независни истраживач и новинар, Суботица, Србија
e-mail: sandra.irsevic@gmail.com

УВОД

Дигитални медији последњих година постали су доминантан простор извештавања о кривичним делима. Вест данас не почиње нити се завршава тренутком објављивања на интернет порталу. Она се допуњује новим детаљима, мења јој се наслов, преноси се на друштвеним мрежама и често се преузима у другим редакцијама без додатне провере. У таквом окружењу црна хроника постаје једна од најчитанијих медијских рубрика, али истовремено и простор у коме се најдиректније сударају право јавности да буде информисана и право појединца да не буде проглашен кривим пре него што о томе одлучи суд, као и право истог тог појединца на приватност и заштиту идентитета.

Предмет овог рада јесте језик наслова и лидова у извештајима домаћих интернет портала о кривичним делима, посматран кроз два међусобно повезана начела: претпоставку невиности и заштиту приватности осумњиченог. Рад полази од тезе да дигитални медији у Србији, у настојању да привуку пажњу публике, наслове често обликују тако да осумњичено лице представе као неспорно утврђеног учиниоца. Тиме се истовремено крши процесно начело претпоставке невиности и недовољно штити приватност лица о коме се извештава.

Рад, уз то, разматра и сродан, али категоријално различит проблем: означавање политичара, јавних функционера и грађана категоричким, криминализујућим изразима у јавном дискурсу, попут речи „лопов”. Циљ поређења ова два феномена, у одељку 4.4, јесте да се прецизно утврди граница између медијске чињеничне тврдње о кривичном делу, на коју се непосредно примењује претпоставка невиности, и политичке критике јавне личности, која ужива шири простор слободе изражавања.

ТЕОРИЈСКИ ОКВИР

Претпоставка невиности као правно начело

Члан 34 став 3 Устава Републике Србије прописује да се свако сматра невиним за кривично дело док се његова кривица не утврди правноснажном одлуком суда (Устав Републике Србије, 2006). Исто начело садржи члан 3 Законика о кривичном поступку (2011). За медијску праксу непосредно је значајан члан 73 Закона о јавном информисању и медијима (2023), којим је прописано да се нико у медију не сме означити учиниоцем кажњивог дела нити огласити кривим или одговорним пре правноснажности одлуке суда. Кодекс новинара и новинарки Србије, чији је издавач Савет за штампу (н.д.), додатно обавезује на заштиту идентитета осумњиченог путем означавања иницијалима и изостављања фотографија и других података који омогућавају препознавање лица, чак и у случају признања кривице, осим када постоји јасан и преовлађујући јавни интерес. Тако се начело претпоставке невиности директно повезује са начелом заштите приватности, па их у пракси није могуће посматрати одвојено.

Теорија медијског уоквиравања и агенда-сетовања

Теорија уоквиравања, коју је систематизовао Роберт Ентман, полази од тога да медији, бирајући поједине аспекте опажене стварности и чинећи их истакнутијим у тексту, обликују

начин на који публика тумачи и вреднује одређени проблем (Entman, 1993). Теорија уоквиравања се применила у анализи текстова, нарочито приликом избора речи којом се осумњичени означава, на пример „осумњичени” наспрам „убица” и присуство или одсуство правне оgrade у наслову представљају конкретне поступке уоквиравања који читаоцу унапред намећу интерпретативни оквир кривице. Класична теорија агенда-сетовања показује да медији не одређују само шта публика мисли, већ и о чему публика уопште размишља, јер избором да одређени случај доспе на насловну страну и остане видљив дуже време, дигитални медији одређују и који ће осумњичени бити предмет најшире јавне пажње, независно од тежине или доказаности дела (McCombs & Shaw, 1972). Оба теоријска приступа примењена су непосредно у одељку 4, где се сваки уочени језички образац тумачи као конкретан поступак уоквиравања.

Концепт „суђења путем медија”

Однос између извештавања у рубрици црне хронике и претпоставке невиности у међународној литератури најчешће се разматра кроз концепт „суђења путем медија” (trial by media), који су развили Крис Греер и Руген МцЛаугхтх анализирајући начин на који медији преузимају функцију суда, изричући јавну пресуду о кривици пре формалног окончања поступка (Greer & McLaughlin, 2011). Према овом приступу, „суђење путем медија” представља тржишно вођен облик популистичке правде у којем се појединци излажу, суде и осуђују у „суду јавног мњења”, при чему медији делују као замена за јавно мњење и преузимају паралелну функцију правосуђа. Наслови попут „Ухапшен убица” или „Пао ‘Врачарац’” не само да преузимају улогу суда пре пресуде, већ и обликују трајну, лако претраживу јавну слику о лицу. Тај ефекат је у дигиталном окружењу знатно израженији него у штампаним медијима на које се првобитно односио овај концепт.

Таблоидизација медија у Србији

Истраживања таблоидизације српских медија показују да је, након 2000. године, дневну штампу у Србији захватио снажан процес таблоидизације, при чему тираж и утицај таблоида наговештавају промене и у новинарским, и у етичким стандардима професионалне заједнице (Миливојевић, 2009). Комерцијална логика клика и видљивости на друштвеним мрежама систематски награђује драматизован, категоричан језик, док опрезније и процесно тачније формулације остају мање видљиве и мање дељене.

Јавне личности, политичари и грађани у јавном дискурсу

Питање да ли се насловима у којима се председник Србије, други функционери или грађани називају „лоповима” могу повезати са претпоставком невиности захтева другачији аналитички приступ од оног који се примењује на осумњичене у кривичном поступку. Претпоставка невиности је најнепосредније релевантна када се одређено лице, у вези са конкретним кажњивим делом и без правноснажне одлуке, представља као његов учинилац.

Ако медиј као сопствену чињеничну тврдњу напише да је одређени функционер „лопов” у смислу да је извршио крађу, злоупотребу положаја, проневеру, примање мита или друго кривично дело, а не постоји правноснажна пресуда, таква формулација може доћи у сукоб са чланом 73 Закона о јавном информисању и медијима.

Другачија је ситуација када медиј верно преноси и јасно приписује политички став одређеном лицу, на пример реченицом „Опозициони лидер оптужио је функционера за крађу” или „Министар је одбацио тврдње да је лопов”. У том случају медиј извештава о постојању политичке изјаве, а не усваја нужно њен садржај као доказану чињеницу. Ипак, ни тада није довољно само механички пренети увреду или оптужбу. Неопходни су јасан извор, контекст и разликовање чињеница од вредносних судова.

Овде је релевантна и пракса Европског суда за људска права, који је у пресуди Лингенс против Аустрије утврдио да су границе прихватљиве критике шире када је реч о политичару него када је реч о приватном лицу, будући да се политичар свесно и неизбежно излаже пажљивом испитивању сваке своје речи и дела од стране новинара и јавности, те мора показати виши степен толеранције (European Court of Human Rights, 1986, para. 42). Овај стандард не значи да јавна функција даје медију дозволу да лице прогласи криминалцем без суда. Он значи да оштра политичка критика и вредносни судови уживају шири простор од чињеничних тврдњи о конкретном кривичном делу.

Приватност и трајност дигиталног садржаја

За разлику од штампаног издања новина, интернет текст остаје доступан у претраживачима и архивама дуго након објављивања. Истраживање Независног удружења новинара Србије указује да накнаде штете које медији плаћају због повреде претпоставке невиности остају ниске и немају одвраћајући ефекат, посебно за таблоиде чији приходи почивају на сензационализму (НУНС, 2024). Кодекс новинара и новинарки Србије налаже заштиту не само имена осумњиченог путем иницијала, већ и других података који омогућавају идентификацију (Савет за штампу, н.д.; Данас, 2024). Истраживање спроведено уз документарни серијал „Доказ” показало је, уз то, да само 30,7% грађана Србије познаје значење претпоставке невиности (Данас, 2017). Ниска свест јавности додатно повећава одговорност медија, будући да за велики део публике управо наслов представља једини извор разумевања појма кривице и невиности.

МЕТОДОЛОГИЈА ИСТРАЖИВАЊА

Предмет, циљ и истраживачка питања

Предмет истраживања је начин на који дигитални медији у Србији, кроз наслове и лидове текстова из рубрике црне хронике, представљају лица осумњичена за извршење кривичних дела. Циљ истраживања је да се утврди да ли се користе правно опрезне формулације, које су најчешће језичке конструкције којима се производи утисак доказане кривичне одговорности, и да ли постоје разлике између портала различитих уређивачких профила.

Истраживачка питања гласе: на који начин портали у Србији језички означавају осумњичене особе; да ли се чешће користе процесно неутралне формулације или формулације које особу представљају као учиниоца; у којој мери сензационалистички изрази доприносе утиску да је кривица већ утврђена и да ли се полицијска саопштења преносе професионално.

Хипотезе истраживања

X1: У насловима текстова чешће него у лидовима користе се формулације које осумњичено лице представљају као учиниоца.

X2: Портали са израженијим таблоидним стилем чешће користе криминализујуће етикете и драматизоване конструкције.

X3: Формулације попут „убица”, „разбојник”, „лопов” и „лажни хирург” представљају индикаторе могућег одступања од претпоставке невиности уколико нису засноване на правноснажној одлуци.

Узорак и корпус

Истраживање је спроведено у две фазе. У првој фази издвојено је 74 јавно доступна текста објављена на седам домаћих онлајн медија: Блиц, Телеграф, Новости, 021, Данас, Информер и Нова.рс. Медији су бирани тако да представљају различите уређивачке профиле у периоду од 1. јануара до 30. јуна 2026. године.

Корпус је обухватио текстове из рубрика црне хронике, друштва и сродних рубрика, који су се односили на хапшење, привођење, истрагу, сумњу, оптужбу или кривични поступак против одређеног лица.

У другој фази примењени су критеријуми за избор текстова за коначну анализу. Издвојена су 34 текста која су испуњавала све услове за укључивање у истраживање: тематску припадност предмету рада, објављивање у утврђеном временском периоду, припадност једном од изабраних домаћих онлајн портала, јасно доступан наслов и лид, као и могућност анализе начина означавања осумњиченог лица, извора информације, присуства или одсуства правне оgrade, језичког стила и заштите идентитета.

Из анализе искључени су дуплирани текстови, збирни дневни прегледи без самосталног случаја, текстови који нису припадали кривичноправној проблематици, текстови о догађајима ван Србије и текстови без јасно доступног наслова или лида. Коначни аналитички узорак чине 34 текста, који су у целини укључени у даљу анализу и кодирани према унапред утврђеној аналитичкој матрици.

Јединицу анализе представља појединачна онлајн објава. Анализирани су наслов и лид текста, док су, када је то било неопходно за тумачење значења, узимани у обзир и извор информације, контекст објављивања, начин означавања лица и подаци који могу омогућити његову идентификацију. Иницијални корпус од 74 текста служио је као полазна документарна грађа, док је 34 текста чинило коначни узорак на којем је спроведена систематска анализа.

При избору нису узимани само примери могућег кршења претпоставке невиности, већ и текстови са неутралнијим формулацијама, како анализа не би била заснована искључиво на унапред издвојеним проблематичним примерима.

Из корпуса су искључени текстови који не припадају хроници или кривичноправној проблематици, збирни дневни прегледи без засебног текста из рубрике црне хронике, текстови о догађајима ван Србије, дуплиране објаве истог портала и текстови без јасно доступног наслова и лида.

Табела 1. Корпус анализираних текстова (N = 34)

Бр	Портал	Датум	Наслов текста (скраћено)	Ниво (0–4)
1	Блиц	26.1.2026.	„Ухапшен убица Живка Бакића: Изрешетао бившег фудбалера Звезде у шуми”	3
2	Блиц	29.1.2026.	„Ојадно Америку за 300 милиона долара”	3
3	Блиц	24.2.2026.	„Детаљи хапшења банде из Новог Пазара”	3
4	Блиц	21.3.2026.	„Ухапшен јеромонах манастира Тресије: Сумња се да је пијан претио игуману”	1
5	Блиц	15.5.2026.	„Ухапшен начелник Београдске полиције Веселин Милић”	0
6	Телеграф	24.2.2026.	„Крвави пир због кутије за донације! Ухапшен разбојник из Жаркова”	4
7	Телеграф	28.2.2026.	„Ово је осумњичени Радомир који је Живка Бакића прво изрешетао по ногама, па га оверио у главу!”	3
8	Телеграф	2.3.2026.	„Ово је осумњичени за убиство Новака Кнежевића у Крагујевцу”	2
9	Телеграф	2.4.2026.	„Пао ‘Врачарац’ у Атини”	3
10	Телеграф	16.6.2026.	„Штаком исекао радницу, другу нокаутирао”	4
11	Новости	6.2.2026.	„Бомба бачена на локал у Новом Београду, двојица ухапшена: Огласио се МУП”	0
12	Новости	23.3.2026.	„Украо 66 клима, па продао: Ухапшен Нишлија”	3
13	Новости	23.4.2026.	„Обећавао операције и узео 100 хиљада евра: Ухапшен Македонац, лажни хирург”	4
14	Новости	28.4.2026.	„Ухапшен осумњичени за убиство на Новом Београду: Чекићем напао човека”	2
15	Новости	15.6.2026.	„Пали због прања новца и пореских превара: Ухапшене четири особе”	3
16	021	7.1.2026.	„Новосадска полиција ухапсила осумњиченог за убиство младића у Товаришеву”	0
17	021	9.3.2026.	„Ухапшен бивши директор ОШ ‘Прва војвођанска бригада’”	3
18	021	23.3.2026.	„Са градилишта у Нишу украо 66 клима уређаја”	3
19	021	14.5.2026.	„Возач осумњичен за покушај убиства”	0
20	021	9.6.2026.	„Ухапшен због 14 крађа: Мештанима Бачке Паланке узео машине и алат”	3
21	Данас	7.2.2026.	„Ухапшен трећи осумњичени за бацање бомбе на кућу Здравка Чолића”	0
22	Данас	11.3.2026.	„Ухапшен због сумње да је оштетио буџет за више од 15 милиона динара”	0
23	Данас	21.4.2026.	„МУП: Ухапшен деветнаестогодишњак који је убио човека у Сремској Митровици и запалио тело”	3
24	Данас	17.5.2026.	„Ухапшен осумњичени за покушај убиства у Врњачкој Бањи”	0
25	Данас	3.6.2026.	„МУП: Ухапшен вођа криминалне групе”	3
26	Информер	19.1.2026.	„Ово је ухапшени Василије Гачевић: Крвнички избо Стефана, био у бекству, па долијао у Шпанији”	4

Бр	Портал	Датум	Наслов текста (скраћено)	Ниво (0–4)
27	Информер	28.1.2026.	„Ухапшен убица Тадије Пантића: Изрешетао вођу навијача, па се скривао два месеца”	4
28	Информер	3.2.2026.	„830 хиљада за едукацију деце спискао на гориво и технику”	2
29	Информер	17.2.2026.	„Ево шта се ставља на терет осумњиченом за паљење аута Баке Прасета”	0
30	Информер	23.5.2026.	„Хитно се огласио МУП: Ухапшен осумњичени за позивање на насилну промену уставног уређења”	0
31	Нова	6.2.2026.	„Ово је осумњичени за убиство предузетнице у Нишу”	2
32	Нова	30.4.2026.	„Ускоро одлука о судбини радника ЈКП Водовод оптужених да су убили Данку Илић”	1
33	Нова	8.5.2026.	„Без повода с леђа ножем напао Немању (19)... Саслушан осумњичени за убиство”	2
34	Нова	5.6.2026.	„Ухапшен осумњичени (26) за убиство у Београду: Оштрим предметом убио мушкарца”	1

Извор: Ауторска анализа података

Аналитичка матрица и ниво скалад

За потребе истраживања конструисана је аналитичка матрица која је обухватила следеће категорије: начин означавања лица, употребу криминализујућих речи, присуство или одсуство правне оградe, извор информације, стил наслова, степен сензационализма и заштиту идентитета.

У односу на начин језичког представљања лица, разликује се пет нивоа поступања према претпоставци невиности. Ниво 0 означава процесно неутралну формулацију, у којој се лице представља као осумњичено, ухапшено или лице против којег постоји сумња, без директног приписивања кривице. Ниво 1 означава делимично опрезну, односно мешовиту формулацију, у којој се процесно неутралан израз комбинује са категоричком тврдњом или драматизованим описом догађаја. Ниво 2 означава имплицитно криминализујућу формулацију, у којој се кривица не износи потпуно директно, али се из избора лексике и структуре наслова може извести закључак о претходно формираном ставу о кривици лица. Ниво 3 означава директно криминализујућу формулацију, у којој се осумњиченом лицу приписује извршење кривичног дела без довољно јасне процесне оградe. Ниво 4 означава директну криминализацију праћену сензационализмом, драматизацијом, експресивном лексиком или детаљима који појачавају утисак већ утврђене кривице.

Поред додељивања једног доминантног нивоа, сваки текст је посебно посматран и у односу на присуство ширих индикатора могућег нарушавања претпоставке невиности. Ови индикатори обухватају изостављање правне оградe, директно означавање лица као учиниоца, употребу криминализујућих именица и глагола, некритичко преношење тврдњи полиције или тужилаштва, сензационалистичко уоквиравање и недовољну заштиту идентитета. На тај начин разликују се доминантни ниво језичке формулације и шири скуп показатеља који могу указивати на нарушавање претпоставке невиности.

У раду се користи формулација „потенцијално нарушавање претпоставке невиности”, а не тврдња да је сваки проблематичан наслов и правно утврђена повреда закона. Ограничење истраживања јесте чињеница да узорак од 34 текста није статистички репрезентативан за све дигиталне медије у Србији, као и да онлајн чланци могу бити накнадно мењани или уклањани.

КВАЛИТАТИВНА АНАЛИЗА И ДИСКУСИЈА

Општи резултати

У коначном аналитичком узорку од 34 текста, у 25 текстова, односно у 73,5% узорка, утврђен је најмање један шири индикатор могућег нарушавања начела претпоставке невиности. Овај податак не представља прост збир текстова разврстаних по нивоима од 0 до 4, јер су укупни индикатори бележени као посебна аналитичка категорија. Један текст је истовремено могао бити сврстан у један доминантни ниво језичког поступања и садржати више додатних индикатора могућег нарушавања.

Добијени резултат показује да се проблем не остварује само кроз директно означавање осумњиченог лица као учиниоца кривичног дела. Он се остварује и комбиновањем више језичких и наративних поступака: изостављањем правне оgrade, употребом категоричних глагола и криминализујућих именица, некритичким преношењем навода полиције или тужилаштва, сензационалистичким уоквиравањем догађаја и недовољном заштитом идентитета лица о којем се извештава. Расподела текстова према доминантном нивоу језичког поступања приказана је у Табели 2.

Табела 2. Расподела анализираних текстова према нивоу језичког поступања

Ниво анализе	Број текстова	Удео у корпусу
0. Процесно неутрална формулација	10	29,4%
1. Делимично опрезна, мешовита формулација	3	8,8%
2. Имплицитно криминализујућа формулација	5	14,7%
3. Директно криминализујућа формулација	10	29,4%
4. Директна криминализација уз сензационализам	6	17,7%
Укупно	34	100%

Извор: Ауторска анализа података

Највећи број текстова, њих 10, сврстан је у ниво 0, што показује да новинари приликом писања текста користе правне оgrade и речи попут ”осумњичени”. Међутим, укупно 24 текста сврстана су у нивое од 1 до 4, што указује на различите степене одступања од потпуно неутралног начина извештавања. Посебно су значајни нивои 3 и 4, који заједно обухватају 16 текстова, односно 47,1% корпуса. У овим текстовима осумњичена лица представљена су директно криминализујућим језиком, често уз додатне елементе сензационализма.

Ови резултати потврђују да наслов има посебно значајну улогу у обликовању интерпретативног оквира. Иако се у самом тексту понекад појављује израз „осумњичени” или формулација „због сумње”, утисак који производи наслов може бити супротан процесној неутралности уколико су у њему већ употребљени глаголи и именице који лицу директно приписују извршење кривичног дела.

Поређење анализираних портала показује разлике у учесталости и интензитету криминализујућих и сензационалистичких формулација. Највиши просечан ниво у анализираном корпусу има портал „Телеграф”, са просечном вредношћу 3,4, док је најнижа просечна вредност забележена код портала „Данас”, са вредношћу 1,2.

Портал „Телеграф” има највећи број текстова са индикаторима могућег нарушавања претпоставке невиности, док „Данас” има најмањи удео таквих текстова у посматраном узорку. Ипак, резултате треба тумачити опрезно, јер је број анализираних текстова по порталу ограничен. Налаз зато указује на тенденције у анализираном корпусу, али не омогућава генерализацију на целокупну продукцију наведених медија.

Добијени резултати подржавају полазну претпоставку о повезаности таблоидног стила и интензивније употребе криминализујуће и драматизоване лексике. Истовремено, присуство проблематичних формулација и на порталима који немају изражен таблоидни профил показује да таблоидизација није једини фактор који утиче на језик извештавања. На избор формулација могу утицати и брзина објављивања, ослањање на институционалне изворе, конкуренција за пажњу публике и уређивачка пракса сваког појединачног медија.

Језички и наративни обрасци

Најизраженији облик проблематичног извештавања, у складу са концептом суђења путем медија јесте употреба речи које осумњичено лице непосредно представљају као учиниоца, попут „убица”, „разбојник”, „банда” или „лажни хирург”. Наслов Информера „Ухапшен убица Тадије Пантића: Изрешетао вођу навијача, па се скривао два месеца” комбинује именицу „убица” са категоричним глаголом „изрешетао” и додатним драматизујућим детаљем о скривању, чиме улази у највиши, четврти ниво анализе и представља модел пресуде изречене пре суда.

Други образац чине категоричне глаголске конструкције без процесне оградe, попут „украо”, „убио” и „запалио”. Наслов Нова „Без повода с леђа ножем напао Немању (19)... Саслушан осумњичени за убиство” у првом делу користи категоричан глагол „напао”, да би тек у наставку увео процесну ограду „осумњичени”, чиме настаје мешовита конструкција слична оној уоченој на порталима Телеграф и Новости.

Портал Данас задржава највећи удео процесно опрезних формулација, али ни он није доследно избегао категоричне формулације попут „МУП: Ухапшен деветнаестогодишњак који је убио човека”. Овај налаз потврђује да ослањање на извор, у овом случају МУП, не ослобађа редакцију обавезе да сама формулација остане процесно тачна.

Осумњичени у извештајима црне хронике наспрам јавних личности у политичком дискурсу

Резултати анализе текстова омогућавају директно поређење са феноменом означавања политичара и функционера криминализујућим изразима. Оба феномена деле површинску сличност, употребу именица попут „лопов” или „убица” за означавање лица пре правноснажне судске одлуке, али се суштински разликују по три критеријума који одређују да ли је начело претпоставке невиности уопште применљиво.

Ово поређење показује да иста реч „лопов” насупротив речи „убица” или „разбојник”, не производи исти правни и етички ризик у сваком контексту. Када редакција сама, без атрибуције, тврди да је конкретно лице извршило конкретно кривично дело, као што показује 29,4% текстова кодираних на трећем нивоу анализе (одељак 4.1), ризик по претпоставку невиности је непосредан и потпуно упоредив без обзира на то да ли је реч о анонимном осумњиченом или о јавном функционеру. Када, међутим, медиј преноси туђу оптужбу или вредносни суд упућен политичару, примењује се шири стандард толеранције критике утврђен у предмету Лингерс против Аустрије. За унапређење истраживања на ове и сличне случајеве предлаже се издвајање и анализа текстова о политичарима, функционерима и грађанима означеним изразима попут „лопов”, са фокусом на разликовање редакцијске чињеничне тврдње од пренесене политичке изјаве.

ЗАКЉУЧАК

Квалитативна анализа 34 текста, издвојена из иницијалног корпуса од 74 текста, показала је да се претпоставка невиности у дигиталном новинарству најчешће доводи у питање начином обликовања наслова и лида. Анализа је указала на присуство различитих степена језичке криминализације, од делимично опрезних и мешовитих формулација до директног означавања осумњичених лица као учинилаца кривичних дела. У 25 од 34 анализирана текста, односно у 73,5% узорка, утврђен је најмање један шири индикатор могућег нарушавања претпоставке невиности. Тај резултат показује да се проблем не може свести само на употребу појединачних речи као што су „убица”, „разбојник”, „лопов” или „лажни хирург”. Од значаја је целокупна структура наслова и лида, укључујући избор глагола, редослед информација, начин представљања извора, присуство правне оgrade и степен сензационалистичке драматизације. Резултати показују да се најизраженија одступања јављају код формулација које осумњиченом лицу директно приписују извршење кривичног дела, иако правноснажна судска одлука још није донета. Посебно су проблематичне конструкције у којима се у наслову употребљава категорична именица или глагол, док се процесна ограда појављује тек у тексту или се уопште не појављује. Таква пракса може створити трајан јавни утисак о кривици лица, нарочито у дигиталном окружењу у којем текстови остају доступни, преносе се на друштвеним мрежама и појављују у претраживачима. Поређење портала указује на већу учесталост и интензитет криминализујућих формулација код портала са израженијим таблоидним стилем. Међутим, резултати истовремено показују да ниједан уређивачки профил није у потпуности изузет од овог проблема. Због ограниченог и намерно одабраног узорка налазе није могуће генерализовати на све дигиталне медије у Србији, али они указују на препознатљив образац који заслужује даља

истраживања на већем и статистички репрезентативнијем корпусу. Посебан допринос рада представља разликовање медијског означавања осумњиченог лица од политичке критике јавне личности. Када редакција сама, као чињеницу, тврди да је одређено лице извршило конкретно кривично дело, непосредно се активира стандард заштите претпоставке невиности из члана 73 Закона о јавном информисању и медијима (2023). Када медиј преноси туђу политичку изјаву и јасно је приписује извору, неопходно је разликовати чињеничну тврдњу од вредносног суда, уз поштовање контекста и права јавних личности на шири простор критике (European Court of Human Rights, 1986). На крају може да се закључи да претпоставка невиности не може да се штити формалним уношењем једне речи као што је „осумњичени”. Неопходно је да наслов, лид и целокупан текст буду формулисани тако да не стварају утисак да је кривица већ утврђена. Одговорно извештавање захтева прецизан језик, јасну атрибуцију извора, доследно коришћење процесних ограда и поштовање приватности лица о којем се извештава.

РЕФЕРЕНЦЕ

Данас. (2017, мај 30). *Само трећина грађана зна шта је претпоставка невиности*. <https://www.danas.rs/vesti/drustvo/samo-trecina-gradjana-zna-sta-je-pretpostavka-nevinosti/>

Данас. (2024, август 13). *Претпоставка невиности или зашто медији и институције „крију” потенцијалне учиниоце кривичних дела иза иницијала?* <https://www.danas.rs/vesti/drustvo/pretpostavka-nevinosti-inicijali/>

Европска конвенција о људским правима. (1950). Члан 6, право на правично суђење. https://www.echr.coe.int/documents/d/echr/convention_ENG

Закон о јавном информисању и медијима. (2023). Члан 73, претпоставка невиности. https://www.paragraf.rs/propisi/zakon_o_javnom_informisanju_i_medijima.html

Законик о кривичном поступку. (2011). Члан 3, претпоставка невиности. https://www.paragraf.rs/propisi/zakonik_o_krivicnog_postupka.html

Миливојевић, С. (2009). *Медији у Србији*. Пешчаник. <https://pescanik.net/mediji-u-srbiji/>

Независно удружење новинара Србије [НУНС]. (2024, мај 22). *Медијске истраге и кршење претпоставке невиности*. <https://nuns.rs/medijske-istrage-i-krsenje-pretpostavke-nevinosti/>

Савет за штампу. (н.д.). *Кодекс новинара и новинарки Србије*. <https://savetzastampu.rs/dokumenta/kodeks-novinara-srbije/>

Устав Републике Србије. (2006). Члан 34, правна сигурност у казненом праву. <https://lexarhiva.rs/propisi/ustav-republike-srbije-2022/drugi-deo/2/clan-34>

Blic.rs. (2026, February 6). *Ovo je ubica žene iz Niša: Sačekaao je ispred kuće i pucao u nju, pre zločina udario komšiju*. <https://www.blic.rs/vesti/hronika/ovo-je-ubica-zene-iz-nisa-sacekao-je-ispred-kuce-i-pucalo-u-nju-pre-zlocina-udario/crnc2c0>

Blic.rs. (2026, February 7). *Duško sa više hitaca ubio Aleksandru, bili u svađi pre ubistva*. <https://www.blic.rs/vesti/hronika/ubistvo-u-nisu-dusko-sa-vise-hitaca-ubio-aleksandru-bili-u-svadji-pre-ubistva/1eleh8v>

Blic.rs. (2026, March 2). *Uhapšen osumnjičeni za ubistvo kod Kragujevca: Izrešetao mladića pred ženom i decom*. <https://www.blic.rs/vesti/hronika/uhapsen-osumnjiceni-za-ubistvo-kod-kragujevca-izresetao-mladica-pred-zenom-i-decom/smgff6d>

Blic.rs. (2026, May 15). *Ovo je spisak svih osam uhapšenih zbog nestanka Aleksandra Nešovića Baje*. <https://www.blic.rs/vesti/hronika/ovo-je-spisak-svih-8-uhapsenih-zbog-nestanka-aleksandra-nesovica-baje/epvk315>

Blic.rs. (2026, May 16). *Hronologija nestanka Aleksandra Nešovića i opsežna akcija hapšenja*. <https://www.blic.rs/vesti/hronika/hronologija-nestanka-aleksandra-nesovica-i-opsezna-akcija-hap-senja/dhckpfd>

Blic.rs. (2026, May 17). *Otkriveno ko je ubio Aleksandra Nešovića: Pucali u njega pred punim restoranom na Senjaku*. <https://www.blic.rs/vesti/hronika/otkriveno-ko-je-ubio-aleksandra-nesovica-u-restoranu-na-senjaku/6nhr39p>

Blic.rs. (2026, May 19). *Uloge u ubistvu Aleksandra Nešovića, upucan zbog jedne rečenice*. <https://www.blic.rs/vesti/hronika/uloge-u-ubistvu-aleksandra-nesovica-upucan-zbog-jedne-recenice/er82h5m>

Blic.rs. (2026, June 13). *Tužilaštvo otkrilo poslednje reči Aleksandra Nešovića pre nego što je ubijen*. <https://www.blic.rs/vesti/hronika/tuzilastvo-otkrilo-poslednje-eci-aleksandra-nesovica-pre-ne-go-sto-je-ubijen-u/6yeygj9>

Cenzolovka. (2026, July 30). *Prorežimski mediji*. <https://www.cenzolovka.rs/tag/prorezimski-mediji/>

Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4), 51–58. <https://doi.org/10.1111/j.1460-2466.1993.tb01304.x>

European Court of Human Rights. (1986). *Case of Lingens v. Austria* (Application no. 9815/82), Judgment of 8 July 1986, para. 42. <https://hudoc.echr.coe.int/fre?i=001-57523>

Greer, C., & McLaughlin, E. (2011). 'Trial by media': Policing, the 24-7 news mediasphere and the 'politics of outrage'. *Theoretical Criminology*, 15(1), 23–46. <https://doi.org/10.1177/1362480610387461>

Informer.rs. (2026, 19. јануар). *Oglasio se deda MMA borca Stefana Savića*. <https://informer.rs/hronika/vesti/1084080/deda-oglasavanje-stefan-savic-ubistvo>

Informer.rs. (2026, 19. јануар). *Ovo je uhapšeni Vasilije Gačević: Krvnički izbo Stefana, bio u bekstvu, pa dolijao u Španiji*. <https://informer.rs/hronika/vesti/1084092/vasilije-gacevic-ubica-mma-borca-stefana-savica>

Informer.rs. (2026, 28. јануар). *Uhapšen ubica Tadije Pantića: Izrešetao vođu navijača, pa se skrivao dva meseca*. <https://informer.rs/hronika/vesti/1086576/uhapsen-osumnjiceni-ubistvo-tadija-pantic>

Informer.rs. (2026, 2. фебруар). *830 hiljada za edukaciju dece spiskao na gorivo i tehniku*. <https://informer.rs/hronika/vesti/1088311/hapsenje-pronevera-novca-pendragon>

Informer.rs. (2026, 6. фебруар). *Uhapšen i treći osumnjičeni za bombaški napad na kuću Zdravka Čolića*. <https://informer.rs/hronika/vesti/1089363/hapsenje-kuca-bomba-zdravko-colic>

Informer.rs. (2026, 17. фебруар). *Evo šta se stavlja na teret osumnjičenom za paljenje auta Bake Praseta*. <https://informer.rs/dzet-set/estrada/1092593/baka-prase-zapaljen-auto-osumnjiceni>

Informer.rs. (2026, 17. фебруар). *Snimak hapšenja osumnjičenog za paljenje auta Bake Praseta*. <https://informer.rs/dzet-set/estrada/1092598/baka-prase-zapaljen-auto-hapsenje-osumnjiceni>

Informer.rs. (2026, 2. март). *Ovako su uhapšeni osumnjičeni za ubistvo Novaka K.* <https://informer.rs/hronika/vesti/1096171/hapsenje-snimak-ubistvo-novak-k-kragujevac>

Informer.rs. (2026, 21. април). *Ovo su ubijena braća u Podgorici: Treća žrtva iz Novog Pazara*. <https://informer.rs/hronika/region/1109109/podgorica-ubijena-braca>

Informer.rs. (2026, 23. мај). *Hitno se oglasio MUP: Uhapšen osumnjičeni za pozivanje na nasilnu promenu ustavnog uređenja*. <https://informer.rs/politika/vesti/1117517/mup-hapsenje-blokader-nasilje>

McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *Public Opinion Quarterly*, 36(2), 176–187. <https://doi.org/10.1086/267990>

Nova.rs. (2026, 6. фебруар). *Ovo je osumnjičeni za ubistvo preduzetnice u Nišu*. <https://nova.rs/vesti/hronika/ovo-je-osumnjiceni-za-ubistvo-preduzetnice-u-nisu-ubio-je-hicama-iz-vatrenog-oruzja-pa-pokusao-da-pobegne-kod-brata-foto/>

Nova.rs. (2026, 30.април). *Uskoro odluka o sudbini radnika JKP Vodovod optuženih da su ubili Danku Ilić*. <https://nova.rs/vesti/hronika/uskoro-odluka-o-sudbini-radnika-jkp-vodovod-optuzenih-da-su-ubili-danku-ilic-2-tragova-i-tela-i-dalje-nema-otkrivamo-sta-se-dogadja-sa-predmetom/>

Nova.rs. (2026, 8.мај). *Bez povoda s leđa nožem napao Nemanju (19), nije ga ni poznao: Saslušan osumnjičeni za ubistvo*. <https://nova.rs/vesti/hronika/bez-povoda-s-ledja-nozem-napao-nemanju-19-nije-ga-ni-poznao-saslusan-osumnjiceni-19-za-ubistvo-na-kanarevom-brdu/>

Nova.rs. (2026, 17.мај). *Dejan je osumnjičene u slučaju nestanka Aleksandra Nešovića Baje odvezao do ovog jezera*. <https://nova.rs/vesti/hronika/osumnjicene-u-slucaju-nestanka-aleksandra-nesovica-baje-odvezao-do-ovog-jezera/>

Nova.rs. (2026, 19.мај). *Otkrivamo šta sve poseduje Saša Vuković Boske koji je uhapšen zbog ubistva Aleksandra Nešovića*. <https://nova.rs/vesti/hronika/otkrivamo-sta-sve-poseduje-sasa-vukovic-boske-koji-je-uhapsen-zbog-ubistva-aleksandra-nesovica-vila-na-senjaku-zemljista-na-cu-karici-firma/>

Nova.rs. (2026, 27.мај). *Ko je imao kakvu ulogu u ubistvu Aleksandra Nešovića Baje?* <https://nova.rs/vesti/hronika/jedan-pucao-drugi-dodavao-pistolj-treci-vozio-osumnjicene-ko-je-ima-ka-kvu-ulogu-u-ubistvu-aleksandra-nesovica-baje-u-restoranu-27/>

Nova.rs. (2026, 5.јун). *Uhapšen osumnjičeni (26) za ubistvo u Beogradu: Oštrim predmetom ubio muškarca*. <https://nova.rs/vesti/hronika/uhapsen-osumnjiceni-26-za-ubistvo-u-beogradu-os-trim-predmetom-ubio-muskarca/>

Nova.rs. (2026, 13.јун). *Tužilaštvo proširilo istragu i otkrilo najnovije detalje ubistva Aleksandra Nešovića u restoranu na Senjaku*. <https://nova.rs/vesti/hronika/sta-se-mrstis-na-svog-brata-tuzilastvo-otkrilo-najnovije-detalle-ubistva-aleksandra-nesovica-u-restoranu-na-senjaku/>

Telegraf.rs. (2026, 28.фeбpуaп). *Ovo je osumnjičeni Radomir (29) koji je Živka Bakića prvo izrešetao po nogama, pa ga overio u glavu*. <https://www.telegraf.rs/vesti/hronika/4280115-ovo-je-osumnjiceni-radomir-29-koji-je-zivka-bakica-prvo-izresetao-po-nogama-pa-ga-overio-u-glavu>

Telegraf.rs. (2026, 2.мaрт). *Ovo je osumnjičeni za ubistvo Novaka Kneževića u Kragujevcu: Lišio ga života pred očima žene i dece*. <https://www.telegraf.rs/vesti/hronika/4281783-ovo-je-ubica-koji-je-brutalno-likvidirao-novaka-knezevica-u-kragujevcu-lisio-ga-zivota-pred-ocima-zene-i-dece>

Telegraf.rs. (2026, 17.мај). *Ovo je Boske koji je osumnjičen da je pucao u Aleksandra Nešovića Baju*. <https://www.telegraf.rs/vesti/hronika/4326221-ovo-je-boske-osumnjicen-da-je-puca-aleksandra-nesovica-baju>

Telegraf.rs. (2026, 1.јун). *Preokret u slučaju Danke Ilić: Sud doneo odluku, osumnjičeni na slobodi*. <https://www.telegraf.rs/vesti/hronika/4335596-preokret-u-slucaju-danke-ilic-sud-doneo-odluku-ko-ja-je-sokirala-srbiju-osumnjiceni-na-slobodi>

Telegraf.rs. (2026, 16.јун). *Osumnjičeni za masakr u Ribnikaru prevario katanac i šifru na koferu punom oružja*. <https://www.telegraf.rs/vesti/hronika/4343910-velikom-mukom-sam-ga-uzeo-osumnjiceni-za-masakr-u-ribnikaru-prevario-katanac-i-sifru-na-koferu-punom-oruzja>

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА, АЛГОРИТМИ И ПРИВАТНОСТ ГРАЂАНА

Јелена Допуђ¹

Сажетак

Убрзани развој вештачке интелигенције и алгоритамских система мења однос грађана према дигиталним медијима и истовремено проширује значење заштите приватности. Корисник у дигиталном окружењу више није само прималац садржаја, већ и извор података који настају његовим претрагама, кликовима, интеракцијама и другим облицима коришћења дигиталних услуга. Повезивањем и анализом таквих података могу да се формирају профили и изводе процене о интересовањима, склоностима и вероватном понашању појединца, укључујући информације које он није непосредно саопштио. Истовремено, алгоритамски системи учествују у селекцији, рангирању и препоручивању садржаја, чиме профил корисника постаје један од фактора који обликују његово информационо окружење. Циљ рада је да анализира везу између дигиталног трага, алгоритамског профилисања, персонализације медијског садржаја и права грађана на приватност. Посебна пажња посвећена је изведеним информацијама, асиметрији знања између корисника и система, ограничењима пристања и транспарентности, као и улози регулаторних и етичких механизма. Полазиште рада је да се приватност у доба вештачке интелигенције не може свести на заштиту већ прикупљених података, већ мора да обухвата и питања начина на који се о појединцу алгоритамски закључује и како се такви закључци користе у дигиталном медијском окружењу.

Кључне речи: вештачка интелигенција, алгоритми, приватност, медији, алгоритамско профилисање, персонализација, подаци о личности

¹ Јелена Допуђ, Новосадски дечји културни центар
e-mail: gogica.gogica@yahoo.com

УВОД

Дигитално медијско окружење значајно је променило начин на који грађани приступају информацијама. Друштвене мреже, претраживачи, мобилне апликације, видео-платформе и друге дигиталне услуге омогућавају готово тренутан приступ великој количини садржаја, али истовремено стварају континуиране токове података о коришћењу тих услуга. Корисник зато више није само прималац информације. Његове претраге, кликови, избори, интеракције и други облици дигиталног понашања могу да постану део ширег скупа података на основу којег се процењују интересовања и преференције, а затим персонализује садржај који ће му бити приказан.

Развој вештачке интелигенције додатно мења природу такве обраде. Савремени алгоритамски системи не служе искључиво за складиштење и систематизацију доступних информација, већ за препознавање образаца, класификацију, предвиђање и подршку у одлучивању. Значај појединачног податка стога више не произлази само из његовог непосредног садржаја. Комбиновањем више података може да се створи нова информација о појединцу, укључујући процену коју он није непосредно саопштио и чије постојање не мора да очекује (Wachter & Mittelstadt, 2019).

Та промена је посебно важна за медије. У традиционалном медијском моделу питање приватности најчешће је било повезано са тим да ли је одређена чињеница о приватном животу лица прикупљена, објављена или учињена доступном јавности.

У дигиталном окружењу, међутим, грађанин може да буде предмет алгоритамске анализе и онда када ниједна нова приватна чињеница није јавно објављена. Профил корисника може да настане повезивањем већ доступних података, а затим да утиче на избор огласа, препорука и садржаја који се том кориснику приказују (Wachter & Mittelstadt, 2019).

На тај начин питање приватности прелази границу класичне тајности података и постаје питање контроле над алгоритамским закључивањем и употребом изведених информација.

Медијска димензија проблема не односи се само на заштиту података корисника. Алгоритми данас учествују и у производњи, селекцији и дистрибуцији медијског садржаја. Пенјишевић и Санчанин указују на ризик да примена вештачке интелигенције у медијском окружењу репродукује или појача постојеће стереотипе и предрасуде, док други радови наглашавају потребу да се техничке могућности АИ посматрају заједно са етичким и критичким аспектима његове употребе у медијском образовању (Penjišević & Sančanin, 2025; Sančanin, Penjišević & Stojanović, 2025).

Предмет овог рада је однос између вештачке интелигенције, алгоритамског профилисања и приватности грађана у дигиталном медијском окружењу. Циљ је да се покаже како се од дигиталног трага долази до изведеног профила корисника, на који начин тај профил може да утиче на персонализацију информационог окружења и због чега заштита приватности више не може да буде сведена само на питање ко поседује податак. Рад је теоријско-аналитичког карактера и заснива се на анализи научне и стручне литературе, релевантних нормативних извора и примера из савременог дигиталног медијског окружења. Регулаторни оквир разматра се као један од механизма заштите, али не и као централни предмет рада.

ОД ДИГИТАЛНОГ ТРАГА ДО АЛГОРИТАМСКОГ ПРОФИЛА

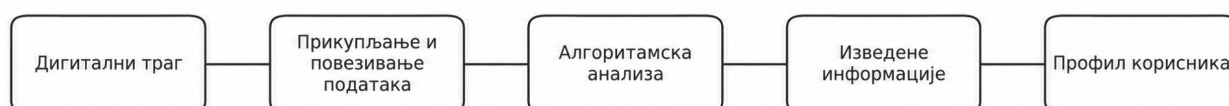
Свакодневно коришћење дигиталних услуга оставља низ података који појединачно могу да изгледају безначајно. Посета одређеној страници, претрага појма, избор видео-садржаја, време задржавања или реакција на објаву сами по себи не морају да откривају много о особи. Њихова вредност се, међутим, мења када се повежу са другим подацима и посматрају током времена. Управо способност повезивања великих количина података и препознавања образаца представља једну од кључних карактеристика савремене алгоритамске анализе.

Wachter и Mittelstadt (2019) указују да аналитика великих података и системи вештачке интелигенције могу да стварају изведене информације и предвиђања о понашању, преференцијама и приватном животу појединаца. Такви закључци не морају да буду интуитивни и кориснику не мора да буде очигледно који податак је имао значај за конкретну процену. На тај начин алгоритамска анализа производи додатни слој информација: поред података које је лице непосредно дало, појављују се и процене које настају њиховим тумачењем.

Алгоритамско профилисање је један од механизма путем којих се овај процес спроводи. Општа уредба о заштити података у члану 4(4) профилисање дефинише као облик аутоматизоване обраде података о личности који се користи ради процене одређених личних аспеката физичког лица, нарочито за анализу или предвиђање аспеката који се односе на радни учинак, економски положај, здравље, личне склоности, интересовања, поузданост, понашање, локацију или кретање (European Parliament and Council, 2016). Значај ове дефиниције није само правни. Она показује да профил није нужно опис већ познатих чињеница, него може да буде процена или предвиђање.

У медијском окружењу та процена има специфичну функцију. Профил корисника може да буде употребљен при одређивању редоследа информација, препоручивању садржаја или избору огласа који ће бити приказан конкретном кориснику (European Parliament and Council, 2022). Због тога се дигитални траг не завршава у бази података. Он може да постане улаз у систем који затим обликује будуће дигитално искуство корисника.

Овде је важно избегавати поједностављење према којем сваки алгоритамски систем „зна” идентитет и намере корисника. Алгоритамски профил може садржати вероватноће, категорије и статистичке процене које су подложне грешци. Управо због тога питање приватности није једино релевантно питање. Нетачна или пристрасна процена може имати последице и када је настала на основу законито прикупљених података. Приватност, тачност података, аутономија и недискриминација у таквим случајевима постају међусобно повезане теме.



Слика 1. Од дигиталног трага до алгоритамског профила

Извор: ауторски приказ на основу Wachter & Mittelstadt (2019) и Adomavicius et al., 2022.

КАДА АЛГОРИТАМ „ЗНА” ОНО ШТО МУ НИСМО РЕКЛИ

Разлика између непосредно датог и изведеног податка једна је од најважнијих за разумевање приватности у доба вештачке интелигенције. Појединац релативно лако може да препозна да је некој услузи оставио име, адресу електронске поште или податак о куповини. Много је теже да зна који се закључци могу извести када се више таквих података повеже са историјом претраживања, интеракцијама или другим доступним сигнаlima.

Wachter и Mittelstadt (2019) овај проблем посматрају као један од важних изазова савременог права заштите података. Према њиховом приступу, постојећи механизми контроле често су снажније усмерени на податке који су прикупљени него на процене које из њих настају. Са становишта грађанина, међутим, последице могу да буду једнако важне. Систем може да формира процену склоности или вероватног понашања, а да лице никада није експлицитно саопштило такву информацију.

Управо зато није довољно поставити само питање „које сам податке дао?”. У алгоритамском окружењу подједнако су важна питања „шта је из тих података закључено?”, „са којим степеном поузданости?” и „за коју сврху се тај закључак користи?”. Разлика је суштинска: чињеница коју је лице саопштило и статистичка процена о њему немају исту природу, али обе могу утицати на начин на који га систем третира (Wachter & Mittelstadt, 2019).

Овакве процене не морају да буду негативне нити су саме по себи недозвољене. Персонализација може кориснику да олакша проналажење релевантног садржаја, смањи количину информација које мора да прегледа и учини дигиталну услугу практичнијом. Проблем се јавља када корисник нема реалну представу о томе да профил постоји, када не зна који су подаци били значајни за његово формирање или када се процена представља као сигурна чињеница иако је у основи само вероватна.

Одатле произлази и питање контроле. Ако је приватност схваћена искључиво као могућност да нека информација остане тајна, из вида се губи ситуација у којој нова информација настаје без непосредног откривања од стране појединца. Савремена заштита приватности зато мора да обухвати и разумност, тачност и легитимност алгоритамских закључака, као и последице њихове употребе (Wachter & Mittelstadt, 2019).

Табела 1. Промена перспективе приватности у алгоритамском окружењу

Класично питање приватности	Питање у алгоритамском окружењу
Које податке сам дао?	Шта је систем из тих података закључио?
Ко има моје податке?	Ко може да их повеже и анализира?
Да ли је податак откривен?	Да ли је створена нова информација о мени?
Ко приступа податку?	Како се профил користи?
Да ли сам пристао на обраду?	Да ли сам могао разумно да предвидим које ће информације бити изведене и како ће бити употребљене?

Извор: ауторски приказ према Wachter & Mittelstadt, 2019.

АЛГОРИТМИ КАО ПОСРЕДНИЦИ ИНФОРМАЦИЈА

У дигиталном медијском окружењу алгоритми имају двоструку улогу. Са једне стране, они анализирају понашање корисника и формирају процене о његовим интересовањима. Са друге стране, исти или повезани системи користе такве процене за рангирање и препоручивање садржаја. Због тога алгоритам није само средство обраде података већ и посредник између корисника и дела информационог простора којем он приступа.

Системи препорука могу да утичу на то који ће се садржај појавити раније, шта ће бити предложено као следеће, који оглас ће бити приказан и које теме ће добити већу видљивост код конкретног корисника. То не значи да алгоритам у потпуности одређује шта грађанин мисли или које информације може да пронађе. Корисник и даље има сопствене изборе, може да претражује садржај и користи различите изворе. Ипак, селекција и редослед информација имају значај јер пажња представља ограничен ресурс, а видљивост садржаја утиче на вероватноћу да ће он бити прочитан, погледан или подељен.

Акт о дигиталним услугама препознаје значај система препорука и захтева од онлајн платформи које их користе да у условима коришћења наведу главне параметре на којима се препоруке заснивају, као и могућности корисника да на те параметре утичу или их измене. Овај захтев је важан управо зато што кориснику омогућава бар делимичан увид у логику по којој се информације селекују и рангирају (European Parliament and Council, 2022).

Исти пропис поставља посебна ограничења оглашавања заснованог на профилисању. Онлајн платформама забрањено је приказивање огласа заснованих на профилисању које користи посебне категорије података о личности. Забрањено је и приказивање огласа заснованих на профилисању уз коришћење података о личности малолетног корисника када платформа са разумном сигурношћу зна да је корисник малолетан (European Parliament and Council, 2022). Ове одредбе показују да европски регулаторни приступ не посматра профилисање само у контексту формалних одлука, већ и као механизам који може да утиче на свакодневно информационо и рекламно окружење грађана.

За медијску професију ово је важна промена. У традиционалном моделу редакција је у великој мери одлучивала о хијерархији вести за све читаоце, гледаоце или слушаоце одређеног медија. У платформском окружењу, до корисника све чешће долази комбинација уреднички произведеног садржаја и алгоритамски посредоване дистрибуције. То значи да исти медијски производ не мора да има исту видљивост код различитих корисника, јер на његову дистрибуцију могу да утичу различити параметри система препорука.

Паралелно са тим, генеративна вештачка интелигенција све више учествује и у производњи и анализи медијског садржаја. У раду о медијској слици Рома у доба вештачке интелигенције указано је на ризик да примена вештачке интелигенције у медијском окружењу репродукује или појача постојеће стереотипе и предрасуде. Истраживање 474 YouTube коментара уз употребу GPT-4 показало је, с друге стране, да велики језички модели могу да убрзају обраду већег скупа текстуалних података, али и да контекстуално, културно и идеолошко тумачење захтева критички људски надзор (Penjišević & Sančanin, 2025; Breazu et al., 2025). Тај пример је важан јер показује да алгоритамски системи нису неутрални посредници изван друштвеног контекста у којем настају и у којем се користе.

ОД ПРОФИЛА КОРИСНИКА ДО ПЕРСОНАЛИЗОВАНОГ ИНФОРМАЦИОНОГ ОКРУЖЕЊА

Однос између података, профила и персонализације најбоље се разуме као циклус. Корисникова реакција на садржај може да постане нови податак, тај податак се поново анализира, профил се ажурира, а наредни избор садржаја може да буде прилагођен новој процени. Тако се ствара повратна спрега у којој је корисник истовремено прималац садржаја и извор сигнала за будућу персонализацију (Adomavicius et al., 2022).

Тај циклус не треба представљати као потпуно затворен систем у којем је сваки наредни избор корисника унапред одређен. На понашање утичу бројни фактори изван платформе, а корисници могу да мењају интересовања, свесно траже различите изворе и одбијају препоруке. Ипак, алгоритамска повратна спрега је важна јер показује зашто једнократни пристанак или једнократна информација о обради података не исцрпљују проблем приватности. Обрада није нужно једнократни догађај, већ динамичан процес у којем се нови подаци стално придружују постојећим.

Управо на овом месту приватност постаје повезана са информационом аутономијом. Ако систем о кориснику континуирано формира процене и користи их за избор садржаја, онда је важно не само да подаци буду технички заштићени, већ и да постоји разумљив увид у то да персонализација постоји, који су њени главни параметри и које могућности корисник има да на њу утиче. Транспарентност овде није пуко објављивање дугачког правног текста, већ услов да корисник може разумно да схвати основни механизам који обликује његово дигитално искуство (European Parliament and Council, 2022).

Овај аспект је посебно значајан за медијску и AI писменост. У раду о унапређењу медијског образовања применом вештачке интелигенције истиче се потреба за интердисциплинарним приступом који, поред разумевања улоге традиционалних и дигиталних медија, обухвата техничке, правне и етичке изазове примене AI (Sančanin, Penjišević & Stojanović, 2025). За грађанина то подразумева и критичко разумевање да персонализовани фид или препорука ни су потпун и неутралан пресек доступних информација, већ резултат избора који је делимично посредован алгоритамским системом.



Слика 2. Алгоритамски циклус персонализације у дигиталном медијском окружењу

Извор: ауторски приказ према Adomavicius et al., 2022.

ПРИВАТНОСТ БЕЗ „ЦУРЕЊА ПОДАТАКА”

У јавним расправама о приватности често доминирају видљиви инциденти: хакерски напад, крађа базе, неовлашћено објављивање података или прослеђивање информација трећем лицу. Такви ризици су несумњиво важни, али алгоритамско окружење показује да проблем приватности може да постоји и без класичног „цурења података”. Податак може да остане у оквиру формално дозвољене обраде, а да се његовим повезивањем ипак изведе нова и осетљива процена о лицу (Wachter & Mittelstadt, 2019).

Један од централних проблема у таквом окружењу јесте асиметрија знања. Организација која располаже великим количинама података и аналитичким алатима може о кориснику да изводи процене које он не види, не разуме или чак не зна да постоје. Корисник може да зна које је појединачне податке оставио, али не мора да зна како су они комбиновани, који су обрасци препознати и колики значај је одређена процена добила у наредном кораку персонализације или одлучивања.

Ова неравнотежа постаје још значајнија када се вероватносна процена третира као стабилна карактеристика личности. Алгоритамски профил није исто што и непосредно утврђена чињеница. Он може да буде непотпун, нетачан или заснован на корелацији која не описује конкретног појединца. Зато заштита приватности треба да буде повезана и са питањем тачности и могућношћу исправке. Ако корисник нема увид у изведену информацију, тешко може да укаже да је она погрешна (Wachter & Mittelstadt, 2019).

Питање пристрасности додатно показује да се приватност не може посматрати изоловано. National Institute of Standards and Technology разликује системску, статистичку и рачунску, као и људску пристрасност и указује да извори пристрасности нису ограничени само на податке и алгоритамске процесе, већ обухватају и институционалне, друштвене и људске факторе (Schwartz et al., 2022). Према томе, није довољно рећи да је „алгоритам пристрасан зато што су подаци пристрасни”. Одговорност се односи на читав процес развоја и примене система.

Медијски контекст показује и други облик ризика. Ако модели за генерисање или класификацију садржаја уче на материјалу који садржи постојеће стереотипе, постоји ризик да се такви обрасци репродукују или појачају. Пењишевић и Санчанин овај проблем разматрају у контексту медијске слике Рома, стереотипа, предрасуда и дискриминације у медијском окружењу (Penjišević & Sančanin, 2025). То не значи да ће сваки модел или сваки резултат бити дискриминаторан, али показује да техничка аутоматизација не уклања друштвени контекст из којег су подаци настали.

МЕДИЈИ, ПЛАТФОРМЕ И ОДГОВОРНОСТ ЗА АЛГОРИТАМСКО ПОСРЕДОВАЊЕ

Промена начина дистрибуције садржаја поставља и питање одговорности медија и платформи. У класичном новинарском моделу уредничка одговорност релативно је видљива: редакција бира тему, одређује приоритет и објављује садржај под својим именом. У платформском окружењу, међутим, пут од објављивања до конкретног корисника укључује и

систем рангирања, препорука и персонализације. Зато је све теже посматрати производњу и дистрибуцију као потпуно одвојене фазе. Садржај може да буде уреднички идентичан, али његова видљивост, учесталост појављивања и контекст у којем се приказује могу да буду различити за различите кориснике (European Parliament and Council, 2022).

То не значи да платформе треба изједначити са редакцијама нити да алгоритамска препорука представља исту врсту уредничке одлуке као избор вести у традиционалном медију. Разлика у улогама остаје важна. Ипак, из перспективе корисника обе врсте селекције утичу на оно што постаје видљиво. Управо зато је корисно разликовати одговорност за настанак садржаја од одговорности за начин његовог алгоритамског рангирања и дистрибуције. Та подела омогућава прецизнију анализу без приписивања алгоритму улоге коју он нема.

Додатни изазов јавља се када медијски актери сами користе системе вештачке интелигенције за анализу публике, оптимизацију наслова, препоруку садржаја или друге облике аутоматизације. Тада питање приватности више није ограничено на велике платформе. Свака организација која користи податке о публици ради профилисања или предвиђања треба да разматра сврху обраде, обим података и реалну потребу за појединим врстама персонализације. Технолошка могућност да се нешто измери или предвиди није сама по себи довољно оправдање да се то и ради (European Parliament and Council, 2016).

Етичка димензија зато постаје важна и онда када је одређена обрада формално дозвољена. Питање није само да ли корисник може да буде профилисан, већ и да ли је начин профилисања сразмеран циљу, довољно транспарентан и усклађен са поштовањем приватности, аутономије и недискриминације (Council of Europe, 2024). У медијском контексту посебно је важно критички размотрити критеријуме оптимизације и последице које они могу имати ако се успех садржаја сведе искључиво на задржавање пажње, број кликова или друге показатеље ангажовања.

Питање одговорности додатно се усложњава чињеницом да у животном циклусу алгоритамског система учествује више актера: програмер, добављач технологије, организација која систем примењује, лице које тумачи резултат и платформа која контролише дистрибуцију. Санчанин, Пењишевић и Бакмаз (2025) у контексту примене AI разматрају и питање приписивања одговорности за његову употребу и могуће проблематичне последице. За медијско окружење тај проблем значи да техничка аутоматизација не укида професионалну и институционалну одговорност, већ захтева јасније разграничење улога.

За медије је важна и чињеница да подаци о публици могу да промене сам процес уредничког одлучивања. Аналитика омогућава редакцијама да виде који садржаји привлаче пажњу, колико се читају и какве реакције изазивају. Такви подаци могу да буду користан сигнал за разумевање интересовања публике, али не би требало да постану једини критеријум уредничке вредности. Ако се одлуке о темама систематски прилагођавају искључиво ономе што алгоритами предвиђа као највероватнији извор ангажовања, постоји ризик да се јавни интерес потисне у корист мерљиве пажње. На тај начин питање података о корисницима постаје повезано и са питањем професионалне аутономије медија.

Истовремено, приватност публике не треба посматрати као препреку развоју дигиталних медија. Подаци могу да помогну у побољшању корисничког искуства, откривању техничких проблема и разумевању начина на који публика приступа садржају. Кључно питање је мера: који су подаци заиста неопходни за конкретну сврху, колико дуго су потребни и да ли се исти циљ може постићи мање интензивном обрадом. Такав приступ одговара принципима ограничења сврхе, минимизације података и ограничења чувања података (European Parliament and Council, 2016).

За јавност је зато важно да постоји јасна разлика између садржаја који је уреднички изабран, садржаја који је алгоритамски препоручен и садржаја који је генерисан или значајно

обрађен системом вештачке интелигенције. Ове категорије могу да се преклапају у пракси, али њихово разликовање доприноси разумевању начина на који информација долази до корисника. То је истовремено питање медијске писмености, професионалне етике и приватности, јер алгоритамска препорука често почива на анализи претходног понашања самог корисника.

ГРАНИЦЕ АЛГОРИТАМСКЕ ОБРАДЕ: ПРАВО, ТРАНСПАРЕНТНОСТ И ОДГОВОРНОСТ

Регулаторни оквир заштите грађана у алгоритамском окружењу развија се на више нивоа. За тему овог рада најважније је да се питање заштите не исцрпљује безбедношћу података, већ обухвата и профилисање, транспарентност, аутоматизовано одлучивање и шире ризике које алгоритамски системи могу да произведу по права појединца. Потреба да се процена утицаја АИ и великих података прошири изван традиционалне заштите података на људска права, друштвене и етичке последице препозната је и у литератури (Mantelero, 2018).

У Републици Србији Закон о заштити података о личности уређује аутоматизовано доношење појединачних одлука и профилисање. Члан 38 предвиђа право лица да се на њега не примењује одлука донета искључиво на основу аутоматизоване обраде, укључујући профилисање, ако она производи правне последице или значајно утиче на његов положај, уз законом предвиђене изузетке и мере заштите. У одређеним случајевима те мере обухватају учешће физичког лица у доношењу одлуке, могућност лица да изрази свој став и право да одлуку оспори (Закон о заштити података о личности, 2018).

Сличан механизам садржи и члан 22 GDPR-а. За предмет овог рада важно је, међутим, нагласити да није свака персонализација медијског садржаја истовремено и аутоматизована одлука са правним или слично значајним последицама. Профилисање и аутоматизовано одлучивање могу се преклапати, али нису истоветни процеси (Article 29 Data Protection Working Party, 2018). Ова разлика спречава преувеличавање правног домета члана 22 и омогућава да се медијска персонализација анализира као посебан проблем приватности и транспарентности, чак и када не достиже праг правно значајне аутоматизоване одлуке.

За платформско медијско окружење посебан значај има Акт о дигиталним услугама, који системима препорука приступа из перспективе транспарентности и избора корисника. Обавеза да се наведу главни параметри препорука показује да је видљивост садржаја постала регулаторно релевантно питање, а ограничења оглашавања заснованог на профилисању посебних категорија података показују да се заштита приватности директно повезује са свакодневним функционисањем платформи (European Parliament and Council, 2022).

Акт о вештачкој интелигенцији уводи шири приступ заснован на ризику и за одређене системе предвиђа захтеве који се односе на управљање ризиком, документацију, транспарентност, људски надзор, тачност, робусност и сајбер-безбедност (European Parliament and Council, 2024). Акценат је, дакле, на промени перспективе: регулаторни фокус се постепено помера са питања шта се дешава са податком ка питању шта може да се догоди са човеком услед употребе система који податке анализира и претвара у процене.

Оквирна конвенција Савета Европе о вештачкој интелигенцији и људским правима, демократији и владавини права међу основним принципима наводи људско достојанство и индивидуалну аутономију, једнакост и недискриминацију, приватност и заштиту података

о личности, транспарентност и надзор, одговорност и поузданост (Council of Europe, 2024). Значај таквог приступа за овај рад је у томе што алгоритамска обрада није сведена на технички проблем, већ се посматра у ширем контексту људских права и стварне могућности погођеног лица да добије релевантне информације и, у одговарајућем контексту, оспори одлуку донету употребом AI система или одлуку која се на њему значајно заснива.

ДА ЛИ ГРАЂАНИН ЗАИСТА КОНТРОЛИШЕ СВОЈЕ ПОДАТКЕ?

Формално постојање права не значи аутоматски и стварну контролу корисника над алгоритамском обрадом. Први проблем јавља се код пристања. Ако лице пристаје на одређену обраду података, али у том тренутку не може разумно да предвиди све будуће комбинације података и изведене процене, поставља се питање колико такав пристајак омогућава реално разумевање касније употребе информација. То не значи да је пристајак као правни основ без значаја, већ да сам по себи не може да реши све проблеме алгоритамског профилисања (Wachter & Mittelstadt, 2019).

Други проблем је транспарентност. Информација има ограничену вредност ако је формално доступна, али је просечном кориснику неразумљива. Сложен опис техничке архитектуре није нужно кориснији од јасног објашњења о томе које се информације користе, за коју сврху и на који начин аутоматизована обрада може да утиче на лице. У том смислу, разумљивост информација треба посматрати као функционални део заштите, а не као административну формалност (Article 29 Data Protection Working Party, 2018).

Трећи проблем односи се на могућност исправке и преиспитивања. Ако алгоритамски профил садржи нетачну процену, корисник тешко може да је исправи ако не зна да она постоји. Код одлука које производе правне последице или на сличан начин значајно утичу на лице, регулаторни оквир предвиђа посебне заштитне механизме, укључујући могућност људске интервенције, изражавања сопственог става и оспоравања одлуке (European Parliament and Council, 2016; Article 29 Data Protection Working Party, 2018). У медијском контексту последице често нису тако директне као код кредита или запошљавања, али питање разумљивости профилисања и даље остаје важно јер персонализација утиче на свакодневно информационо окружење.

У том простору важну улогу имају AI и медијска писменост. У раду о примени вештачке интелигенције у медијском образовању наглашава се да разумевање AI не треба ограничити на техничке могућности алата, већ га повезати и са правним, етичким и критичким аспектима његове употребе (Sančanin, Penjišević & Stojanović, 2025). Грађанин треба да разуме да препорука није исто што и уредничка процена, да персонализовани фид није потпун пресек доступних информација и да алгоритамска процена није нужно непогрешива.

Ипак, одговорност за заштиту приватности не сме да буде пребачена искључиво на појединца. Захтев да сваки грађанин у потпуности разуме сложене алгоритамске системе био би нереалан, посебно када начин рада, извор података или релативни значај појединих параметара нису непосредно видљиви. AI и медијска писменост могу повећати способност појединца да препозна ризик, али не могу заменити обавезе организација које системе развијају и примењују, нити потребу за јасним регулаторним и етичким стандардима.

Зато се одржив однос између алгоритамске ефикасности и права на приватност не може свести на избор једног од ова два интереса. Питање није да ли треба користити алгоритамске системе или штитити приватност, већ под којим условима је њихова употреба оправдана, транспарентна и подложна стварној контроли. У медијском окружењу такав приступ подразумева и одговорност платформи и медијских актера, јасније разликовање уредничких и алгоритамских механизма селекције и посебну пажњу у ситуацијама у којима профилисање може да продуби постојеће неједнакости.

ЗАКЉУЧАК

Примена вештачке интелигенције мења начин на који приватност грађана треба разумети у дигиталном медијском окружењу. Заштита више није ограничена на податке које је појединац непосредно оставио, уступио или учинио доступним. Алгоритамски системи могу да повезују различите податке, препознају обрасце и на основу њих формулишу профиле, процене и предвиђања која садрже информације које лице никада није непосредно саопштило. Управо способност алгоритамског закључивања представља један од кључних изазова савремене заштите приватности. У дигиталним медијима тај изазов добија додатну димензију јер се профили не користе само за формалне одлуке. Они могу да утичу на избор, редослед и препоруку садржаја, па корисник истовремено постаје извор података и прималац информација чија је видљивост делимично обликована на основу претходног понашања. Због тога алгоритамска персонализација није само техничко питање ефикасније дистрибуције садржаја, већ и питање транспарентности, аутономије и контроле над информацијама које се о појединцу изводе. Ризик не настаје самим постојањем алгоритма нити је свака персонализација проблематична. Значај имају сврха и обим обраде, врста података, начин формирања профила, поузданост изведених закључака и последице њихове употребе. Посебан изазов представља асиметрија знања између организација које располажу великим количинама података и грађана који не морају да знају које су процене о њима формиране. У таквом окружењу приватност не може да буде сведена на питање да ли је база података безбедна или да ли је дошло до неовлашћеног откривања информације. Европски регулаторни оквир и домаће право препознају ову промену кроз правила о профилисању, аутоматизованом одлучивању, системима препорука, транспарентности и управљању ризицима. Ипак, нормативне гаранције имају стварну вредност само ако су разумљиве и оствариве. Када се обрада заснива на пристанку, његова практична вредност је ограничена ако корисник не може разумно да предвиди шта ће бити изведено из његових података, а транспарентност губи смисао ако се сведе на информацију коју просечан корисник не може да разуме. Зато кључно питање приватности у доба вештачке интелигенције више није само које податке о нама неко поседује. Подједнако је важно шта из тих података може да закључи, са којим степеном поузданости, како ће тај закључак употребити и какве последице он може да има по наше информационо окружење и положај. Заштита грађана мора да прати читав пут информације – од дигиталног трага, преко алгоритамског повезивања и профилисања, до начина на који профил утиче на препоруке, садржај и одлуке. У том смислу, право на приватност у доба вештачке интелигенције подразумева не само заштиту податка од неовлашћеног приступа, већ и очување разумне контроле над начином на који се о појединцу алгоритамски закључује.

РЕФЕРЕНЦЕ

- Adomavicius, G., Bockstedt, J. C., Curley, S. P., & Zhang, J. (2022). Recommender systems, ground truth, and preference pollution. *AI Magazine*, 43(2), 177–189. <https://doi.org/10.1002/aaai.12055>
- Breazu, P., Schirmer, M., Hu, S., & Katsos, N. (2025). Large Language Models and the challenge of analyzing discriminatory discourse: human-AI synergy in researching hate speech on social media. *Journal of Multicultural Discourses*, 19(3), 157–175. <https://doi.org/10.1080/17447143.2025.2476967>
- Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). Strasbourg: Council of Europe.
- Article 29 Data Protection Working Party. (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01).
- European Parliament and Council. (2016). Regulation (EU) 2016/679 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 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.
- European Parliament and Council. (2022). Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, L 277, 1–102.
- European Parliament and Council. (2024). Regulation (EU) 2024/1689 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). *Official Journal of the European Union*, L, 2024/1689.
- Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, 34(4), 754–772. <https://doi.org/10.1016/j.clsr.2018.05.017>
- Penjišević, A., & Sančanin, B. (2025). Media Image of Roma in the Age of Artificial Intelligence. *KNOWLEDGE – International Journal*, 73(1), 223–229.
- Sančanin, B., Penjišević, A., & Bakmaz, O. (2025). The use of artificial intelligence in the recruitment process. *Conference on Social and Technological Development*, 14, 39–46. <https://doi.org/10.63395/STEDConf14022025910S39>
- Sančanin, B., Penjišević, A., & Stojanović, K. (2025). Improving media education through the application of artificial intelligence. *International Scientific Conference on Economics, Management and Information Technologies*, 2(1), 249–254. <https://doi.org/10.71159/icemit2529S>
- Schwartz, R., Vassilev, A., Greene, K. K., Perine, L., Burt, A., & Hall, P. (2022). Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. NIST Special Publication 1270. <https://doi.org/10.6028/NIST.SP.1270>
- Закон о заштити података о личности. (2018). Службени гласник РС, бр. 87/2018.
- Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 2019(2), 494–620. <https://doi.org/10.7916/cblr.v2019i2.3424>

МЕДИЈСКА ПИСМЕНОСТ И СВЕСТ ГРАЂАНА СРБИЈЕ О ЗАШТИТИ ПРИВАТНОСТИ У ДИГИТАЛНОМ ОКРУЖЕЊУ: АНАЛИЗА ДОСТУПНИХ ПОКАЗАТЕЉА

Ђорђе Возаревић¹

Сажетак

Развој дигиталних медија, друштвених мрежа и онлајн платформи довео је до све интензивнијег прикупљања, обраде и размене личних података грађана. У таквом окружењу медијска писменост не подразумева само способност приступања, разумевања и критичког вредновања медијских садржаја, већ и познавање начина функционисања дигиталних платформи и механизма заштите приватности. Предмет рада је однос између медијске писмености и свести грађана Србије о ризицима којима су њихови лични подаци изложени у дигиталном окружењу. Циљ рада је анализа доступних нормативних, статистичких и стручних показатеља који могу указати на степен информисаности грађана, њихово познавање права и примену практичних мера заштите. Посебна пажња посвећена је разлици између опште забринутости за приватност и стварног понашања корисника, као и улози медија, образовних институција и надлежних органа у развијању културе заштите личних података. Полази се од претпоставке да интензивно коришћење дигиталних медија није нужно праћено одговарајућим нивоом критичког разумевања начина прикупљања и употребе личних података.

Кључне речи: медијска писменост, приватност, лични подаци, дигитални медији,

¹ Институт за филозофију и интердисциплинарне студије, Нови Сад, Србија
e-mail: djole.vozarevic@gmail.com

УВОД

Дигитализација комуникације, развој друштвених мрежа, онлајн медија, мобилних апликација и услуга заснованих на вештачкој интелигенцији променили су начин на који грађани приступају информацијама, успостављају односе, учествују у јавном животу и задовољавају свакодневне потребе. Истовремено, готово свака активност у дигиталном окружењу оставља одређени траг: податке о идентитету корисника, његовој локацији, интересовањима, навикама, претрагама, контактима и начинима коришћења медијских садржаја. Лични подаци тако постају значајан ресурс дигиталне економије, док њихово прикупљање, повезивање и обрада отварају питања контроле, надзора, профилисања и могуће злоупотребе.

Право на приватност и заштиту података о личности припада основним правима грађана, али његово остваривање у дигиталном окружењу не зависи искључиво од постојања правних прописа и поступања надлежних институција. Оно у значајној мери зависи и од способности појединаца да препознају ризике, разумеју начине на које дигиталне платформе користе њихове податке и примене одговарајуће мере заштите. У Републици Србији Закон о заштити података о личности уређује права физичких лица у вези са обрадом података, обавезе руковалаца и обрађивача, надзор над применом закона, као и правна средства и одговорност у случају повреде права. Ипак, постојање нормативног оквира само по себи не обезбеђује висок ниво заштите уколико грађани нису упознати са својим правима и начинима њиховог остваривања (Закон о заштити података о личности, 2018). У том контексту медијска писменост добија шире значење од способности приступања медијским садржајима и њиховог критичког тумачења. Она обухвата и разумевање технолошких, економских и алгоритамских механизма на којима се заснива функционисање савремених медија и дигиталних платформи. Медијски писмен грађанин требало би да буде способан да процени не само веродостојност одређеног садржаја већ и последице остављања личних података, прихватања дозвола апликација, омогућавања праћења локације, коришћења подразумеваних подешавања приватности и објављивања информација о себи и другим лицима. Европски оквир дигиталних компетенција DigComp 3.0 зато заштиту личних података и приватности сврстава у област безбедног, одговорног и критичког коришћења дигиталних технологија (Cosgrove & Cachia, 2025).

Значај овог питања посебно је изражен имајући у виду распрострањеност употребе интернета у Србији. Према подацима Републичког завода за статистику, у 2025. години интернет прикључак поседовало је 90,1% домаћинстава, док је интернет користило 90% лица обухваћених истраживањем. Више од 89% корисника приступало је интернету више пута током дана. Ови подаци указују на висок степен укључености грађана у дигитално окружење, али распрострањеност приступа и учесталост употребе не морају истовремено означавати и развијеност критичких знања и вештина неопходних за заштиту приватности (Републички завод за статистику, 2025). На постојање несразмере између забринутости грађана и њихове информисаности указују и резултати домаћих истраживања. Други талас истраживања *Перцепција грађана о заштити података о личности*, спроведен 2023. године на узорку од 1.211 пунолетних грађана Србије, показао је да грађани ову област сматрају важном, али да нису у довољној мери упознати са терминологијом, сопственим правима и начинима институционалне заштите. Чак 80% испитаника оценило је ризик од злоупотребе личних података као висок, док је 56,7% сматрало да јавност није довољно обавештена о заштити података о личности. Само 19,9% испитаника сматрало је да је јавност у довољној мери информисана (Kantar Serbia & TMG Insights, 2023).

Истраживање медијске писмености грађана Србије из 2025. године додатно показује да део грађана нема развијене практичне способности за управљање приватношћу. Праћење локације знало је да искључи 55,7% испитаника, а праћење дигиталне активности 52,2%. Мање од половине испитаника, односно 48,4%, сматрало је да уме да процени када је безбедно поделити личне податке, док је само 14% навело да зна како да се заштити од онлајн превара, укључујући крађу идентитета, фишинг и финансијске преваре. Наведени резултати показују да свакодневна употреба дигиталних медија није нужно праћена одговарајућим нивоом знања и практичних вештина заштите (Матовић и др., 2025).

Предмет овог рада јесте однос између медијске писмености и свести грађана Србије о заштити приватности у дигиталном окружењу. Циљ рада је да се, анализом релевантне научне и стручне литературе, правног оквира, статистичких података и резултата доступних истраживања, сагледају ниво информисаности грађана, њихово познавање ризика и права, као и практични облици понашања у заштити личних података. Полази се од претпоставке да постоји несразмера између интензивног коришћења дигиталних медија и степена оспособљености грађана да препознају ризике и предузму конкретне мере заштите приватности. У раду се примењују анализа садржаја, секундарна анализа резултата постојећих истраживања и интерпретативна метода, уз посебно разматрање улоге медија, образовних установа и надлежних институција у развијању културе заштите личних података.

МЕДИЈСКА ПИСМЕНОСТ КАО КОМПЕТЕНЦИЈА САВРЕМЕНОГ ГРАЂАНИНА

Медијска писменост представља једну од основних компетенција грађана у савременом информационом друштву. Њен значај произлази из чињенице да медији више нису само средства преношења информација, већ важни чиниоци обликовања ставова, вредности, идентитета и друштвених односа. У условима убрзане дигитализације грађани се свакодневно сусрећу са великим бројем информација, медијских порука, огласа, алгоритамски препоручених садржаја и различитих захтева за уступање личних података. Због тога способност техничког коришћења дигиталних уређаја није довољна за одговорно и безбедно учешће у медијском окружењу. У литератури се медијска писменост најчешће одређује као способност приступања медијским садржајима, њихове анализе и критичког вредновања, као и стварања сопствених порука у различитим комуникацијским контекстима. Ливингстонова наглашава да приступ, анализа, вредновање и стварање садржаја представљају међусобно повезане компоненте медијске писмености. Појединац, дакле, није медијски писмен само зато што уме да приступи одређеном садржају или користи одређену платформу. Он мора бити способан и да препозна начин на који је порука конструисана, интересе који стоје иза њеног настанка и могуће последице њеног прихватања или даљег ширења (Livingstone, 2004).

Појам медијске писмености током времена проширен је са традиционалних штампаних и аудиовизуелних медија на интернет, друштвене мреже, претраживаче, мобилне апликације и друге дигиталне платформе. Такво проширење било је неопходно јер се положај корисника у дигиталном окружењу значајно променио. Грађанин више није само прималац медијских порука већ истовремено може бити њихов аутор, дистрибутер, коментатор и предмет

прикупљања података. Његове активности могу се бележити и анализирати чак и када он активно не објављује садржаје, на основу претрага, кликова, времена задржавања, локације, контаката и других облика дигиталног понашања. Отуда се медијска писменост не може свести само на препознавање лажних вести, пропаганде или манипулативног садржаја. Она обухвата и разумевање власничке структуре медија, економских интереса, начина финансирања платформи, алгоритамског избора садржаја и комерцијалне вредности података о корисницима. У том смислу медијска писменост подразумева способност појединца да препозна сопствени положај у систему у којем се његова пажња, навике и лични подаци могу претварати у економски ресурс. Заштита приватности зато није издвојена техничка или правна област, већ саставни део критичког разумевања савременог медијског система. Овакво схватање присутно је и у Европском оквиру дигиталних компетенција DigComp 3.0, у којем је заштита личних података и приватности издвојена као посебна компетенција у области безбедности. Она подразумева познавање и остваривање права у вези са личним подацима, препознавање ризика, одговорно и етичко коришћење података, као и подешавање начина њиховог прикупљања и дељења. Оквир показује да дигитална компетентност није само питање оперативног знања већ обухвата критичко размишљање, безбедност, одговорност и свест о последицама употребе технологије (Cosgrove & Cachia, 2025).

UNESCO такође повезује медијску и информациону писменост са заштитом приватности. Поред способности приступања, анализе и стварања информација, медијски писмен грађанин треба да разуме начине на које медији, технолошке компаније и друге институције управљају подацима. То укључује способност процене политика приватности, препознавање монетизације личних профила и разумевање чињенице да се коришћење наизглед бесплатних дигиталних услуга често заснива на прикупљању и анализирању података корисника. Медијска писменост на тај начин омогућава грађанима да доносе информисаније одлуке о томе које податке ће уступити, коме, у коју сврху и под којим условима (UNESCO, 2021). Посматрано из социолошке перспективе, медијска писменост није искључиво индивидуална способност, већ је условљена друштвеним положајем, образовањем, старошћу, материјалним могућностима и доступношћу институционалне подршке. Различите друштвене групе немају једнак приступ знању и ресурсима неопходним за безбедно коришћење дигиталних медија. Формална доступност интернета стога не значи да сви грађани имају једнаке способности да процене ризике, заштите податке или остваре своја права. Ливингстонова указује да је медијска писменост повезана са расподелом знања и способности у друштвено раслојеној популацији, као и са институционалним управљањем моћи коју доносе приступ информацијама и способност њихове употребе (Livingstone, 2004). Посебан проблем представља разлика између декларативног знања и стварног понашања корисника. Грађани могу сматрати приватност важном и истовремено прихватати услове коришћења без читања, користити исте лозинке на више места, јавно објављивати личне информације или давати апликацијама дозволе које нису неопходне за њихов рад. У литератури се ова несагласност између изражене забринутости и стварног поступања означава као „парадокс приватности”. Истраживања показују да корисници често уступају податке када непосредну корист, погодност или приступ услузи процене као важније од могућег, временски удаљеног ризика (Barth & de Jong, 2017).

Медијска писменост, међутим, не би требало да пребаци целокупну одговорност за заштиту приватности на појединца. Корисници се често суочавају са сложеним и неразумљивим политикама приватности, унапред одабраним подешавањима, честим захтевима за пристанак и техничким решењима чије последице нису лако уочљиве. Због тога је, поред развијања индивидуалних компетенција, неопходна и одговорност медија, дигиталних платформи, образовних установа, државних органа и регулаторних институција. Савет Европе медијску

и информациону писменост посматра као део ширег одговора на изазове које дигитално медијско окружење поставља пред људска права, демократију и владавину права (Council of Europe, 2026). На основу наведеног, медијски писмен грађанин може се одредити као активан и критички субјект који разуме природу медијских порука, препознаје интересе и механизме који обликују дигитално окружење и уме да управља сопственим присуством и подацима у том окружењу. Заштита приватности зато представља један од показатеља стварног нивоа медијске писмености. Она се не огледа само у знању о постојању одређених ризика већ и у способности да се то знање примени кроз промишљено дељење информација, контролу подешавања, процену захтева за приступ подацима и коришћење доступних механизма заштите.

ПРИВАТНОСТ И ПОДАЦИ О ЛИЧНОСТИ У ДИГИТАЛНОМ МЕДИЈСКОМ ОКРУЖЕЊУ

Приватност представља једну од основних претпоставки личне аутономије, достојанства и слободног развоја појединца. Она подразумева могућност човека да одређује у којој мери ће информације о њему бити доступне другим лицима, институцијама и организацијама. У савременом друштву приватност се, међутим, више не односи само на физички и породични простор, тајност преписке или заштиту од непосредног надзора. Развој дигиталних медија проширио је ово питање на прикупљање, чување, повезивање, анализирање и размену података насталих током свакодневног коришћења интернета. Право на приватност и право на заштиту података о личности међусобно су повезана, али се не могу у потпуности изједначити. Приватност је шири појам који обухвата различите области личног и породичног живота, док се заштита података о личности односи на правила и поступке којима се уређује обрада информација повезаних са одређеним физичким лицем. Према Закону о заштити података о личности Републике Србије, податак о личности јесте сваки податак који се односи на физичко лице чији је идентитет одређен или одредив. То значи да податак о личности није само име и презиме, адреса или јединствени матични број већ и свака информација која, самостално или у комбинацији са другим информацијама, може довести до идентификације одређеног лица (Закон о заштити података о личности, 2018). Право на заштиту података о личности представља важан део права на приватност и у Србији је гарантовано Уставом и посебним законом (Устав Републике Србије, 2006/2021; Закон о заштити података о личности, 2018). Поред непосредних идентификационих података, у дигиталном окружењу прикупљају се и бројни технички и бихејвиорални подаци. Они могу обухватити интернет адресу уређаја, идентификатор мобилног телефона, податке о локацији, историју претраживања, посећене странице, време задржавања на садржајима, куповне навике, контакте, реакције на објаве и начин кретања кроз апликације. Појединачни податак понекад не омогућава непосредно утврђивање идентитета, али његовим повезивањем са другим подацима може настати веома детаљна слика о одређеном кориснику (Закон о заштити података о личности, 2018).

У том смислу може се говорити о активном и пасивном дигиталном трагу. Активни дигитални траг настаје када корисник свесно објављује фотографије, коментаре, податке о образовању, запослењу, интересовањима или тренутној локацији. Пасивни дигитални траг настаје прикупљањем података које корисник не уноси непосредно, као што су подаци о

уређају, времену приступа, кретању, претрагама и интеракцијама са садржајем. Граница између ова два облика није увек јасна, јер корисник може добровољно приступити одређеној услузи, а да при томе не разуме у потпуности обим података који се о њему прикупљају (UNESCO, 2021). Посебно место у процесу прикупљања података имају колачићи и сличне технологије праћења. Колачићи су мале датотеке које интернет страница поставља на уређај корисника како би омогућила одређене функције, запамтила изборе или пратила коришћење странице. Неопходни технички колачићи могу бити потребни за функционисање сајта, док аналитички и маркетиншки колачићи омогућавају праћење активности и повезивање података ради мерења понашања или приказивања персонализованих огласа. Повереник као једно од начела обраде истиче минимизацију података, односно прикупљање само оних података који су неопходни за одређену сврху (European Data Protection Board [EDPB], 2020; Закон о заштити података о личности, 2018).

Обимно прикупљање података омогућава профилисање корисника. Профилисање подразумева аутоматизовану обраду података ради процене или предвиђања личних особина, интересовања, понашања, економског положаја, кретања или склоности одређеног лица (Article 29 Data Protection Working Party, 2018). На основу тако формираног профила платформе могу одређивати које ће садржаје, огласе, препоруке или понуде корисник видети. Европски одбор за заштиту података профилисање и аутоматизовано одлучивање издваја као посебно значајна питања за остваривање права лица чији се подаци обрађују. Алгоритамска персонализација може олакшати проналажење релевантних информација, али истовремено смањује транспарентност медијског окружења. Корисник најчешће нема потпун увид у то на основу којих података је одређени садржај изабран, зашто му је приказан одређени оглас и које су претпоставке о њему изведене из претходног понашања. На тај начин подаци не служе само описивању корисника већ и усмеравању његове пажње, избора и будућег понашања. Питање приватности зато постаје и питање односа моћи између појединца и организација које располажу технолошким средствима за масовно прикупљање и анализу података (EDPB, 2021). Један од основних правних услова за поједине облике обраде јесте пристанак лица на које се подаци односе. Да би био ваљан, пристанак мора бити добровољан, одређен, информисан и недвосмислен, а лице мора имати могућност да га опозове (Закон о заштити података о личности, 2018; EDPB, 2020). Међутим, у пракси се корисници често суочавају са дугим и сложеним правилима приватности, нејасно формулисаним обавештењима и интерфејсима који подстичу брзо прихватање свих понуђених опција. Европски одбор за заштиту података упозорава на обмањујућа дизајнерска решења на друштвеним платформама, којима се корисници усмеравају ка одлукама које нису нужно у складу са њиховим стварним интересима и жељама. Пример таквог поступања може бити наглашено дугме за прихватање свих колачића, док је могућност одбијања сакривена иза већег броја корака. Сличан проблем постоји када је приступ садржају условљен прихватањем обраде која није неопходна за пружање саме услуге. У таквим ситуацијама формално изражен пристанак не мора значити да је корисник заиста разумео сврху, обим и последице обраде. Због тога се свест о приватности не може мерити само спремношћу грађана да означе одређено поље или притисну дугме „прихватам”, већ и њиховом способношћу да процене шта прихватање конкретно подразумева.

Ризици за приватност не настају искључиво деловањем великих платформи. Грађани могу угрозити сопствену или туђу приватност прекомерним објављивањем података, фотографија, докумената и информација о локацији. Посебан проблем представља објављивање података о другим лицима без њихове сагласности. Једном објављен садржај може бити копиран, прослеђен, архивиран или употребљен изван првобитног контекста, чак и када је накнадно уклоњен са профила. Последице могу обухватити нежељено откривање идентитета, нарушавање

угледа, дискриминацију, крађу идентитета, превару или друге облике злоупотребе (UNESCO, 2021). Осетљивост података не зависи само од њиховог формалног назива већ и од контекста у којем се користе. Наизглед безначајне информације могу, када се повежу, открити навике, друштвене односе, здравствено стање, политичке ставове, верска уверења или друге аспекте приватног живота. Због тога савремена заштита података почива на начелима законитости, транспарентности, ограничења сврхе, минимизације података, тачности, ограниченог чувања, безбедности и одговорности онога ко податке обрађује (Закон о заштити података о личности, 2018).

Заштита приватности у дигиталном окружењу не може се свести на потпуно повлачење корисника из онлајн комуникације. У друштву у којем су информисање, образовање, пословање, јавне услуге и друштвени односи у великој мери дигитализовани, потпуно избегавање остављања података готово је немогуће. Циљ заштите није онемогућавање протока података, већ успостављање услова у којима се они обрађују законито, оправдано, транспарентно и уз поштовање достојанства и права појединца. Конвенција Савета Европе број 108 била је први правно обавезујући међународни инструмент у области заштите података, док њена модернизована верзија настоји да одговори на изазове нових информационих и комуникационих технологија и прекограничног преноса података (Council of Europe, 1981, 2018). Са становишта медијске писмености, кључно питање није само да ли грађани знају да се њихови подаци прикупљају већ да ли разумеју ко их прикупља, у коју сврху, колико дуго их чува, са ким их дели и какве закључке на основу њих може изводити. Стварна свест о приватности подразумева повезивање знања, критичке процене и практичног поступања. Грађанин који декларативно сматра приватност важном, али без размишљања прихвата све захтеве, јавно објављује осетљиве информације и не користи доступна подешавања заштите, не показује у потпуности развијену компетенцију управљања приватношћу. Управо ће разлика између ставова, знања и стварног понашања бити једно од основних полазишта за анализу свести грађана Србије у наставку рада.

ПРАВНИ И ИНСТИТУЦИОНАЛНИ ОКВИР ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ

Заштита приватности и података о личности у Републици Србији заснива се на уставним гаранцијама, посебном законодавству, међународним стандардима и деловању надлежних институција. Постојање правног оквира има посебан значај у дигиталном окружењу, у којем се подаци грађана прикупљају и обрађују у великом обиму, често аутоматизовано и без непосредног увида лица на које се односе. Међутим, ефикасност правне заштите не зависи само од квалитета прописа већ и од тога у којој мери грађани познају своја права и умеју да користе расположиве механизме заштите. Устав Републике Србије у члану 42 изричито јемчи заштиту података о личности. Прикупљање, држање, обрада и коришћење података уређују се законом, док је употреба података изван сврхе за коју су прикупљени забрањена и кажњива, осим у случајевима предвиђеним законом. Устав такође гарантује право сваког лица да буде обавештено о подацима који су о њему прикупљени и право на судску заштиту у случају њихове злоупотребе. Тиме је заштита података о личности постављена као самостално уставно

право, повезано са људским достојанством, аутономијом и приватним животом појединца (Устав Републике Србије, 2006, чл. 42). Основни пропис у овој области представља Закон о заштити података о личности, усвојен 2018. године, чија је примена почела у августу 2019. године. Законом се уређују начела обраде података, права лица на која се подаци односе, обавезе руковалаца и обрађивача, пренос података у друге државе и међународне организације, надзор над спровођењем закона, правна средства, одговорност и казне. Закон се примењује на аутоматизовану обраду, као и на неаутоматизовану обраду података који чине део одређене збирке или су намењени да постану њен део (Закон о заштити података о личности, 2018, чл. 1–3).

Законитост обраде не подразумева само формално постојање одређеног правног основа. Обрада мора бити поштена и транспарентна, спроведена у одређене, изричите и оправдане сврхе, а прикупљени подаци морају бити примерени, релевантни и ограничени на оно што је неопходно (Закон о заштити података о личности, 2018, чл. 5). Подаци треба да буду тачни, безбедно чувани и задржани само онолико дуго колико је потребно за остварење сврхе обраде. Руковалац подацима има обавезу да поштује ова начела и да буде у могућности да докаже да поступа у складу са законом. Овај принцип одговорности посебно је значајан у односу на дигиталне платформе, медије, јавне институције, трговинска предузећа и друге субјекте који обрађују велики број података грађана. Грађанима је законом признат низ права којима могу остварити већу контролу над својим подацима. Она обухватају право на информисање о обради, приступ подацима, исправку нетачних и допуну непотпуних података, брисање у законом предвиђеним случајевима, ограничење обраде, преносивост података и подношење приговора. Посебна права односе се на аутоматизовано доношење одлука и профилисање када таква одлука производи правне последице или значајно утиче на одређено лице (Закон о заштити података о личности, 2018, чл. 23–40). Грађанин, дакле, није само пасивни предмет обраде већ носилац права који може захтевати информације и интервенцију у начину на који се његови подаци користе. Значајно место у законском систему има пристанак лица на које се подаци односе. Пристанак мора бити добровољан, одређен, информисан и недвосмислен, а лице има право да га опозове. Ипак, пристанак није једини могући правни основ обраде. Подаци се, под законом прописаним условима, могу обрађивати и ради извршења уговора, испуњења правне обавезе, заштите животно важних интереса, обављања послова у јавном интересу или остваривања легитимног интереса. Када се обрада заснива на пристанку, он мора бити јасно исказан, а лице мора имати могућност да га опозове (Закон о заштити података о личности, 2018, чл. 12 и 15). Због тога медијска писменост подразумева и разумевање да свако појављивање обавештења о приватности или дугмета „прихватам” не значи нужно да је обрада заснована на стварно слободном и информисаном избору корисника. Централну институционалну улогу има Повереник за информације од јавног значаја и заштиту података о личности, као самосталан и независан државни орган. У области заштите података Повереник надзире примену закона, поступа по притужбама грађана, спроводи инспекцијски надзор, даје мишљења и смернице, упозорава руковооце на неправилности и предузима законом предвиђене корективне мере (Закон о заштити података о личности, 2018, чл. 73–79). Грађанин који сматра да је обрада његових података извршена супротно закону може се најпре обратити руковооцу ради остваривања својих права, а затим поднети притужбу Поверенику или затражити судску заштиту (Закон о заштити података о личности, 2018, чл. 82–84).

Посебан значај за предмет овог рада има однос између заштите приватности и слободе јавног информисања. Медији имају право и обавезу да објављују информације о питањима за која постоји оправдан интерес јавности, али слобода информисања није неограничена. Закон о јавном информисању и медијима уређује објављивање информација о личности,

заштиту достојанства, приватног живота и права лица на која се информације односе, као и средства правне заштите. Приликом објављивања личних података неопходно је успоставити равнотежу између интереса јавности да буде информисана и права појединца на приватност. Постојање радозналости публике само по себи не представља оправдан јавни интерес (Закон о јавном информисању и медијима, 2023/2025, чл. 91–93). Одговорност медија не огледа се само у избегавању незаконитог објављивања података. Медији имају и образовну функцију, јер начин на који извештавају о крађи идентитета, дигиталним преварама, злоупотреби фотографија, надзору и профилисању може утицати на разумевање ових појава. Закон о јавном информисању и медијима у јавни интерес укључује развој медијске, информационе и дигиталне писмености, као и производњу садржаја којима се унапређују људска права и слободан развој личности. Тиме се ствара нормативна основа да медији активно учествују у подизању свести грађана о заштити приватности, а не само да се уздржавају од њеног нарушавања (Закон о јавном информисању и медијима, 2023/2025, чл. 15–16). Шири институционални приступ утврђен је Стратегијом заштите података о личности за период од 2023. до 2030. године. За њено спровођење усвојен је Акциони план за период од 2025. до 2027. године, којим су предвиђене нормативне измене, јачање институционалних капацитета и активности усмерене ка ефикаснијем остваривању права грађана (Стратегија заштите података о личности, 2023; Акциони план за спровођење Стратегије, 2025). Усвајање ових докумената указује на то да се заштита података не може обезбедити само појединачним поступцима по притужбама, већ захтева дугорочну и координисану јавну политику. Иако грађанима Србије стоји на располагању релативно развијен систем правних права и институционалних механизма, његова практична вредност зависи од доступности и разумљивости информација. Лице које не зна који субјект обрађује његове податке, која права има и коме може да се обрати тешко може делотворно користити законску заштиту. Стога правна писменост у области заштите података представља саставни део медијске и дигиталне писмености. Познавање закона не мора подразумевати детаљно познавање свих правних норми, већ способност грађанина да препозна могућу повреду, затражи објашњење, оствари своја права и обрати се надлежној институцији.

ПОКАЗАТЕЉИ СВЕСТИ ГРАЂАНА СРБИЈЕ О ЗАШТИТИ ПРИВАТНОСТИ

Процена свести грађана о заштити приватности захтева истовремено разматрање више показатеља: степена изложености дигиталном окружењу, информисаности о прикупљању и обради података, процене ризика, познавања права и институција, као и практичних способности заштите. Висока учесталост коришћења интернета сама по себи не сведочи о развијеној медијској писмености. Она, пре свега, показује да је велики део становништва свакодневно изложен ситуацијама у којима се лични подаци остављају, прикупљају и обрађују. Према подацима Републичког завода за статистику, у 2025. години широкопојасни интернет имало је 90,1% домаћинстава у Србији, док је интернет користило 90% лица узраста од 16 до 74 године. Налог на друштвеним мрежама имало је 84,7% интернет популације (Републички завод за статистику [РЗС], 2025). Ови подаци показују да је дигитална комуникација постала

уобичајен део свакодневног живота већине грађана, чиме се истовремено повећава број ситуација у којима корисници откривају личне податке, прихватају услове коришћења или остављају трагове свог понашања. За сагледавање односа грађана према приватности посебно су значајна два новија истраживања. Истраживање *Перцепција грађана о заштити података о личности* спроведено је 2023. године на стратификованом узорку од 1.211 пунолетних грађана Србије из урбаних и руралних подручја (Kantar Serbia & TMG Insights, 2023). Истраживање *Медијска писменост грађана Србије* реализовано је од 15. маја до 15. јуна 2025. године на двоетапном стратификованом репрезентативном узорку од 800 испитаника узраста од 18 до 75 година (Матовић и др., 2025). Резултати оба истраживања заснивају се претежно на самопроцени испитаника, што значи да их треба тумачити као показатеље ставова, перцепција и пријављених способности, а не као потпуно објективно мерење практичног знања.

Забринутост грађана и процена ризика

Резултати истраживања из 2023. године показују да грађани заштиту података о личности сматрају важном, али да истовремено процењују да нису довољно упознати са овом облашћу. Ризик од угрожавања или злоупотребе података као висок оценило је 80% испитаника. Истовремено, 39,8% сматрало је да своје податке штити у умереној мери, док је 28,9% оценило да их штити у великој мери или у потпуности (Kantar Serbia & TMG Insights, 2023). Наведени резултати показују да је забринутост за приватност широко распрострањена, али не омогућавају закључак да је праћена одговарајућим знањем и понашањем. Грађани могу бити свесни да злоупотреба података представља опасност, а да при томе не умеју да препознају све облике прикупљања података, да процене законитост њихове употребе или да примене конкретне мере заштите. Стога је потребно разликовати општу свест о постојању ризика од оперативне способности управљања приватношћу. Више од половине испитаника, односно 56,7%, сматрало је да јавност није довољно обавештена о заштити података о личности, док је 23,3% било неодлучно. Само 19,9% оценило је да је јавност довољно информисана. Поред тога, 48,3% грађана сматрало је да доступне информације о заштити података нису довољно јасне, а свега 20,5% да су оне јасне (Kantar Serbia & TMG Insights, 2023).

Ови подаци упућују на то да проблем није само у количини доступних информација већ и у њиховој разумљивости. Правила приватности, обавештења о обради података и законска објашњења често су написани стручним или техничким језиком. Уколико грађанин не може да разуме сврху обраде, рок чувања података или права која му припадају, формална доступност информације не доводи нужно до стварне информисаности.

Препознавање повреда приватности

Одређени резултати показују да значајан део грађана препознаје конкретне облике нарушавања приватности. Објављивање фотографија или видео-снимака других лица на друштвеним мрежама без њихове сагласности као повреду података о личности препознало је 75,5% испитаника. Објављивање имена дужника као проблем је препознало 61,3%, снимање запослених ради контроле временаведеног на раду 62%, а постављање видео-надзора тако да снима улаз у туђи стан или кућу 52,7% испитаника (Kantar Serbia & TMG Insights, 2023). Разлике у одговорима уочене су и према образовању и месту становања. Испитаници са средњим и високим образовањем чешће су од оних са завршеном основном школом препознавали да објављивање туђих фотографија без сагласности представља повреду приватности. Поједине облике повреде чешће су препознавали и становници градских средина (Kantar Serbia & TMG Insights, 2023). Овај налаз потврђује да свест о приватности није једнако развијена у свим друштвеним групама. Образовање, приступ информацијама, искуство у коришћењу технологије и друштвено окружење могу утицати на способност грађана да препознају ризичне ситуације. Заштита приватности стога није искључиво питање личне одговорности већ и питање неједнаке расподеле знања и дигиталних компетенција.

Практичне способности заштите приватности

Истраживање медијске писмености из 2025. године показује да су поједине основне дигиталне вештине присутне код нешто више од половине грађана. Праћење сопствене локације знало је да искључи 55,7% испитаника, док је 52,2% навело да уме да искључи праћење дигиталног понашања, као што је историја прегледања. Блокирање или брисање другог корисника са листе пријатеља умело је да изврши 54,9% испитаника (Матовић и др., 2025). Сложеније способности заштите знатно су слабије развијене. Само 48,4% корисника интернета сматрало је да уме да процени у којим ситуацијама може безбедно да подели приватне податке, док је 51,6% навело да то не уме или није сигурно да уме. Свега 14% испитаника тврдило је да зна како да се заштити од онлајн превара, као што су крађа идентитета, нежељене поруке, фишинг и изнуда новца. Искључивање меморије система вештачке интелигенције знало је да изврши 17,5% испитаника (Матовић и др., 2025). Разлика између способности искључивања једноставних техничких функција и способности процене сложенијих ризика указује на неуједначен ниво медијске и дигиталне писмености. Део грађана уме да употреби одређену команду или промени подешавање, али нема довољно знања да процени у којим околностима је уступање података оправдано, које последице може имати и како да препозна обману. Ови резултати потврђују разлику између техничке оспособљености и критичке дигиталне компетенције. Техничка оспособљеност подразумева способност коришћења уређаја и апликација, док критичка компетенција укључује разумевање економских и алгоритамских механизма прикупљања података, процену ризика и доношење информисаних одлука.

Познавање права и институционалних механизма

Један од најизраженијих проблема односи се на недовољно познавање права. Чак 62% испитаника сматрало је да грађани нису упознати са својим правима у области заштите података о личности, док је 29,1% било неодлучно. Само 8,8% оценило је да су грађани донекле или веома добро упознати са својим правима (Kantar Serbia & TMG Insights, 2023). Недовољна информисаност видљива је и у избору институције којој би се грађани обратили у случају неовлашћене обраде података. Више од половине испитаника, односно 55,7%, прво би се обратило полицији, док би се 28% обратило Поверенику за информације од јавног значаја и заштиту података о личности, а 5,8% тужилаштву. Око 10,5% испитаника не би се обратило никоме (Kantar Serbia & TMG Insights, 2023). Чињеница да би се већина грађана најпре обратила полицији, а не органу специјализованом за заштиту података, може указивати на недовољно познавање надлежности институција. То не значи да обраћање полицији у свакој ситуацији мора бити погрешно, посебно уколико постоје елементи кривичног дела, али показује да значајан део грађана не препознаје Повереника као примарни механизам заштите у случају незаконите обраде података. Посебно је значајан налаз да би се испитаници који су видели или чули за кампању „Нека остане лично” Поверенику обратили у већем проценту од оних који нису били упознати са кампањом - 48,9% према 26% (Kantar Serbia & TMG Insights, 2023). Истовремено, грађани који нису били упознати са кампањом чешће би се обратили полицији. Ова разлика показује да јавне кампање могу имати практичан значај, јер не утичу само на општу видљивост теме већ и на познавање конкретних институционалних механизма. Међутим, са самом кампањом било је упознато свега 8,8% испитаника, што указује на ограничен домет појединачних и временски ограничених активности информисања (Kantar Serbia & TMG Insights, 2023).

Разлика између ставова и понашања

Синтеза резултата показује постојање изражене несразмере између декларативне забринутости за приватност и практичне способности њене заштите. Са једне стране, већина грађана ризик од злоупотребе података оцењује као висок и сматра да је заштита података важна. Са друге стране, мање од половине уме да процени када је безбедно поделити приватне податке, веома мали број зна како да се заштити од онлајн превара, а већина сматра да грађани нису упознати са својим правима (Kantar Serbia & TMG Insights, 2023; Матовић и др., 2025). Ова несагласност може се тумачити као облик парадокса приватности: појединци изражавају забринутост, али њихове навике, знања и избори нису увек у складу са таквим ставом (Barth & de Jong, 2017). Ипак, одговорност се не може приписати само корисницима. На поступање грађана утичу сложена правила приватности, нејасна обавештења, подразумевана подешавања, дизајн платформи и чињеница да је приступ одређеним услугама често условљен уступањем података (European Data Protection Board, 2023). Резултати доступних истраживања зато указују да свест грађана Србије о приватности постоји пре свега на нивоу опште забринутости и препознавања појединих ризика, али је слабије развијена на нивоу критичког разумевања, практичних вештина и познавања права. То потврђује полазну претпоставку рада да интензивно коришћење дигиталних медија није нужно праћено одговарајућим нивоом медијске писмености и способности заштите личних података.

УЛОГА МЕДИЈСКЕ ПИСМЕНОСТИ У УНАПРЕЂЕЊУ ЗАШТИТЕ ПРИВАТНОСТИ

Резултати доступних истраживања показују да грађани Србије у значајној мери препознају општу опасност од злоупотребе личних података, али да су њихова практична знања, познавање права и способност процене конкретних ризика недовољно развијени. Због тога унапређење заштите приватности не може бити сведено само на доношење прописа или техничко обезбеђивање дигиталних система. Оно захтева континуирано развијање медијске, информационе, дигиталне и правне писмености грађана (Kantar Serbia & TMG Insights, 2023; Матовић и др., 2025). Медијска писменост може допринети заштити приватности пре свега тако што грађанима омогућава да разумеју природу савременог дигиталног медијског окружења. Корисник треба да буде свестан да друштвене мреже, претраживачи, информативни портали и мобилне апликације не функционишу само као средства комуникације, већ и као системи за прикупљање, анализу и комерцијалну употребу података. Зато образовање о приватности не би требало да се сведе на опште упозорење да личне податке не треба делити са непознатим лицима. Потребно је објаснити на који начин настаје дигитални траг, како функционишу колачићи и дозволе апликација, шта је алгоритамско профилисање и како се на основу података кориснику прилагођавају огласи и медијски садржаји (UNESCO, 2021; EDPB, 2021). Посебан значај има образовни систем. Садржаји о заштити приватности треба да буду укључени у наставу медијске и дигиталне писмености, грађанског васпитања, информатике и других сродних предмета. Ученици не би требало само да усвоје дефиниције личних података већ и да кроз практичне примере науче како се подешава приватност налога, како се препознају покушаји преваре, које дозволе апликација нису неопходне и какве последице може имати објављивање туђих фотографија или података без сагласности (Cosgrove & Cachia, 2025; UNESCO, 2021). Поред ученика, потребно је континуирано усавршавати наставнике, јер се технолошки услови и облици дигиталних ризика брзо мењају.

Образовне активности не треба ограничити само на децу и младе. Доступна истраживања указују на разлике у дигиталним компетенцијама према старости, образовању и месту становања. Зато су потребни програми намењени одраслима, старијим лицима, становницима руралних средина и другим групама које могу имати мањи приступ обукама и стручним информацијама (Kantar Serbia & TMG Insights, 2023; Матовић и др., 2025). Такви програми треба да буду практични, бесплатни или лако доступни и прилагођени стварним ситуацијама са којима се грађани сусрећу приликом коришћења електронске трговине, друштвених мрежа, електронског банкарства и јавних дигиталних услуга. Медији такође имају значајну улогу у развијању свести о приватности. Поред извештавања о случајевима злоупотребе података, медији могу грађанима објашњавати како да препознају ризике и коме да се обрате у случају повреде права. Вест о крађи идентитета, неовлашћеном објављивању фотографије или злоупотреби базе података има већи образовни значај уколико садржи јасно објашњење начина на који је до повреде дошло, права оштећеног лица и доступних механизма заштите. У том смислу, медији не би требало само да региструју последице већ и да доприносе превенцији (Закон о јавном информисању и медијима, 2023/2025, чл. 15–16). Истовремено, медији морају поштовати приватност лица о којима извештавају. Објављивање имена, фотографија, здравствених података, породичних околности или других информација из приватног живота мора бити оправдано стварним јавним интересом. Посебан опрез неопходан је када

су у питању малолетници, жртве насиља, пацијенти и друга осетљива лица (Закон о јавном информисању и медијима, 2023/2025, чл. 91–93). Медиј који кроз своје садржаје промовише медијску писменост, а истовремено неоправдано открива личне податке, шаље противречну поруку јавности и слаби поверење у професионалне стандарде. Надлежне институције треба да обезбеде да информације о правима буду лако доступне, разумљиве и прилагођене различитим категоријама грађана. Подаци из анализираног истраживања показују да велики број грађана не препознаје јасно надлежности институција у области заштите података. Већина би се у случају неовлашћене обраде најпре обратила полицији, док би се знатно мањи део обратио Поверенику за информације од јавног значаја и заштиту података о личности (Kantar Serbia & TMG Insights, 2023). Због тога су потребне дугорочне, а не само повремене кампање, које би објасниле шта представља повреду права, како се подноси захтев руковооцу, у којим ситуацијама се подноси притужба Поверенику и када је потребно обратити се полицији, тужилаштву или суду.

Комуникација институција треба да избегава претежно правни и стручни језик, посебно имајући у виду да готово половина испитаника доступне информације о заштити података не сматра довољно јасним (Kantar Serbia & TMG Insights, 2023). Кратка упутства, видео-материјали, примери из свакодневног живота и јасно представљени кораци за остваривање права могу бити делотворнији од обимних докумената које већина грађана не чита. Посебно је важно да се информације о заштити података редовно објављују на местима на којима грађани већ проводе време, на друштвеним мрежама, информативним порталима и платформама јавних институција.

Организације цивилног друштва, библиотеке, школе, факултети и локалне самоуправе могу допринети ширењу знања кроз радионице, јавне трибине, саветовалишта и локалне медијске кампање. Њихова улога посебно је важна у срединама у којима су институционални ресурси ограничени. Сарадња различитих актера омогућила би да се заштита приватности не третира само као питање стручњака за право и информационе технологије, већ као тема од непосредног значаја за свакодневни живот грађана (Council of Europe, 2026). Развијање индивидуалних компетенција не сме довести до пребацивања целокупне одговорности на корисника. Дигиталне платформе и други руковооци подацима имају обавезу да обезбеде транспарентна обавештења, разумљиве услове коришћења и подешавања приватности која корисника не усмеравају ка одлукама супротним његовим интересима (Закон о заштити података о личности, 2018; EDPB, 2023). Заштита приватности треба да буде уграђена у дизајн дигиталне услуге, а не представљена као додатна могућност коју корисник мора самостално да пронађе и активира. Унапређење заштите приватности, према томе, захтева поделу одговорности између грађана, образовних институција, медија, државних органа и технолошких компанија. Улога медијске писмености јесте да грађанима омогући да доносе информисане и критички промишљене одлуке, али и да препознају када је њихово право повређено и захтевају одговорност других актера. На тај начин медијска писменост постаје не само средство личне заштите већ и услов активног грађанства и равноправног учешћа у дигиталном друштву.

ПРЕПОРУКЕ ЗА УНАПРЕЂЕЊЕ СВЕСТИ ГРАЂАНА О ЗАШТИТИ ПРИВАТНОСТИ

На основу анализираних показатеља може се закључити да унапређење свести грађана Србије о заштити приватности захтева систематско и координисано деловање образовних установа, медија, надлежних институција, организација цивилног друштва и дигиталних платформи. Посебну пажњу треба усмерити на повезивање општег знања о ризицима са практичним вештинама и познавањем механизма правне заштите (Kantar Serbia & TMG Insights, 2023; Матовић и др., 2025). Пре свега, теме које се односе на приватност, личне податке, дигитални траг, профилисање и безбедно понашање треба систематски укључити у програме медијске и дигиталне писмености на свим нивоима образовања. Настава не би требало да буде заснована искључиво на усвајању појмова, већ и на практичним вежбама које обухватају подешавање приватности, контролу дозвола апликација, препознавање фишинга, заштиту налога и процену оправданости захтева за уступање личних података (Cosgrove & Cachia, 2025; UNESCO, 2021). Потребно је развити и програме неформалног образовања за одрасле и старије грађане, као и за становништво у мањим и руралним срединама, имајући у виду разлике у знању и дигиталним способностима различитих друштвених група (Kantar Serbia & TMG Insights, 2023; Матовић и др., 2025). Такве обуке могу се организовати у библиотекама, школама, домовима културе, локалним самоуправама и организацијама цивилног друштва. Садржаји треба да буду прилагођени конкретним потребама корисника и ситуацијама са којима се они сусрећу у свакодневном животу.

Надлежне институције треба да унапреде начин информисања грађана о њиховим правима, посебно имајући у виду да значајан део грађана није довољно упознат са механизмима институционалне заштите (Kantar Serbia & TMG Insights, 2023). Објашњења о томе како се остварује право на приступ, исправку, брисање или ограничење обраде података треба представити једноставним и разумљивим језиком (Закон о заштити података о личности, 2018, чл. 23–40). Посебно је важно јасно објаснити разлику између надлежности Повереника, полиције, тужилаштва и суда, како би грађани у случају повреде приватности знали коме треба да се обрате.

Јавне кампање о заштити података треба да буду континуиране и присутне у различитим медијима, а не ограничене на повремене активности. Резултати истраживања показују да познавање одређене кампање може бити повезано са бољим препознавањем надлежне институције, али и да је домет таквих активности и даље ограничен (Kantar Serbia & TMG Insights, 2023). Због тога је потребан дугорочан и стратешки приступ информисању различитих група грађана (Council of Europe, 2026). Поред телевизије, радија и штампаних медија, неопходно је користити друштвене мреже, видео-садржаје, подкасте и друге формате прилагођене начину на који се различите старосне групе информишу. Кампање треба да садрже конкретне примере повреда приватности и јасна упутства за поступање. Медији би требало да развијају специјализоване садржаје о дигиталним правима, онлајн преварама, злоупотреби личних података и алгоритамском профилисању, чиме би допринели остваривању јавног интереса у области медијске, информационе и дигиталне писмености (Закон о јавном информисању и медијима, 2023/2025, чл. 15–16). Истовремено, медији морају доследно поштовати приватност лица о којима извештавају и избегавати објављивање података који нису неопходни за остваривање јавног интереса (Закон о јавном информисању и медијима, 2023/2025, чл. 91–93).

Дигиталне платформе и други субјекти који обрађују податке треба да обезбеде јасна и лако доступна подешавања приватности. Обавештења о обради података морају бити разумљива и транспарентна, док избор корисника не сме бити усмеравањем обмањујућим дизајнерским решењима (Закон о заштити података о личности, 2018; EDPB, 2023). Подразумевана подешавања требало би да обезбеде виши, а не најнижи ниво заштите приватности. Неопходно је редовно спроводити истраживања медијске писмености и свести грађана о приватности на репрезентативним узорцима. Имајући у виду да се постојећи резултати у значајној мери заснивају на одговорима и самопроцени испитаника, будућа истраживања требало би да укључе и практичне задатке којима би се провериле стварне способности грађана (Kantar Serbia & TMG Insights, 2023; Матовић и др., 2025). Коначно, заштиту приватности треба развијати као заједничку друштвену одговорност. Од грађана се може очекивати опрезно и информисано поступање, али само у окружењу у којем су правила јасна, институције доступне, медији одговорни, а дигиталне услуге пројектоване тако да поштују права корисника.

ЗАКЉУЧАК

Ширење дигиталних медија довело је до тога да питање приватности више не припада искључиво правној или техничкој области. Оно је постало саставни део свакодневне комуникације, информисања, куповине, образовања и коришћења јавних и комерцијалних услуга. Грађани се у таквом окружењу непрекидно налазе у ситуацији да остављају податке о себи, али најчешће немају потпун увид у путеве њихове даље употребе, повезивања и тумачења. Анализа доступних истраживања показала је да међу грађанима Србије постоји изражено осећање угрожености и свест да злоупотреба података може имати озбиљне последице. Ипак, таква забринутост није у истој мери праћена сигурношћу у поступању. Посебно су уочљиве тешкоће у процени када је безбедно уступити податке, препознавању сложенијих дигиталних претњи, разумевању алгоритаМСког праћења и познавању институција којима се грађани могу обратити. Тиме је потврђена полазна претпоставка да учестало коришћење интернета и дигиталних платформи не подразумева аутоматски и способност одговорног управљања сопственом приватношћу. Налази такође указују на то да свест о заштити података није јединствена и непроменљива категорија. Она обухвата знање, ставове, практичне навике и спремност да се права стварно употребе. Грађанин може препознати да одређени поступак представља опасност, а да истовремено не уме да промени подешавања, процени веродостојност захтева или покрене поступак заштите. Због тога се стварни ниво оспособљености не може процењивати само на основу изражене бриге, већ и према конкретним одлукама и понашању у дигиталном простору. Медијска писменост у том смислу добија улогу посредника између формално гарантованих права и њиховог остваривања у пракси. Њен задатак није само да упозори на опасности, већ да омогући разумевање начина на који функционишу платформе, пословни модели засновани на подацима, системи препорука и механизми профилисања. Истовремено, она треба да оспособи грађане да препознају границе дозвољене обраде, критички процене захтеве за приступ подацима и реагују када сматрају да су њихова права повређена. Међутим, ни највиши ниво индивидуалне оспособљености не може у потпуности надокнадити нетранспарентне поступке организација које располажу подацима. Зато унапређење заштите приватности захтева истовремено деловање на више нивоа: разумљивије институционалне

информације, континуирано образовање, одговорније медијско извештавање, јаснија правила дигиталних услуга и подешавања која корисника не доводе у неповољан положај. Посебну пажњу треба посветити групама које због старости, образовања, места становања или ограниченог приступа обукама имају мање могућности да развију потребне компетенције. Заштита приватности стога не треба да се посматра као изолован лични задатак, већ као показатељ квалитета дигиталног грађанства и односа друштва према људском достојанству. Само повезивањем знања, институционалне подршке и одговорности оних који прикупљају податке могуће је створити окружење у којем грађани неће бити само корисници дигиталних услуга, већ обавештени носиоци права способни да утичу на услове сопственог присуства у дигиталном простору.

РЕФЕРЕНЦЕ

Article 29 Data Protection Working Party. (2018). *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (WP251rev.01). Endorsed by the European Data Protection Board on 25 May 2018 (Accessed: August 9, 2025).

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior—A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. doi: 10.1016/j.tele.2017.04.013 (Accessed: August 9, 2025).

Cosgrove, J., & Cachia, R. (2025). *DigComp 3.0: European Digital Competence Framework* (5th ed.). Luxembourg: Publications Office of the European Union. doi: 10.2760/0001149, JRC144121 (Accessed: August 9, 2025).

Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108). Strasbourg: Council of Europe (Accessed: August 9, 2025).

Council of Europe. (2018). *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (CETS No. 223). Strasbourg: Council of Europe (Accessed: August 7, 2025)..

Council of Europe. (2026). *National Media and Information Literacy Strategies: Practical Steps and Indicators*. Strasbourg: Council of Europe (Accessed: August 7, 2025)..

European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*. Brussels: European Data Protection Board (Accessed: August 12, 2025)..

European Data Protection Board. (2021). *Guidelines 8/2020 on the targeting of social media users*. Brussels: European Data Protection Board (Accessed: August 12, 2025)..

European Data Protection Board. (2023). *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: How to recognise and avoid them* (Version 2.0) (Accessed: August 9, 2025)..

European Data Protection Board. (2023). *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: How to recognise and avoid them* (Version 2.0). Brussels: European Data Protection Board.

Kantar Serbia & TMG Insights. (2023). *Перцепција грађана о заштити података о личности: Други талас истраживања јавног мњења*. Београд: Повереник за информације од јавног значаја и заштиту података о личности и Мисија ОЕБС-а у Србији.

Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review*, 7(1), 3–14. doi: 10.1080/10714420490280152.

UNESCO. (2021). *Media and information literate citizens: Think critically, click wisely! Media and information literacy curriculum for educators and learners. Part 2, Module 8: Privacy, data protection and you*. Paris: UNESCO.

Акциони план за период од 2025. до 2027. године за спровођење Стратегије заштите података о личности за период од 2023. до 2030. године. „Службени гласник РС”, бр. 20/2025.

Закон о заштити података о личности. „Службени гласник РС”, бр. 87/2018.

Закон о јавном информисању и медијима. „Службени гласник РС”, бр. 92/2023 и 51/2025.

Матовић, М., Милојевић, А., Милин Перковић, С., Томашевић, А., Јосифовић, С., и Јовић, М. (2025). *Медијска писменост грађана Србије: Извештај анкетног истраживања*. Београд: Мисија ОЕБС-а у Србији.

Републички завод за статистику. (2025). *Употреба информационо-комуникационих технологија у Републици Србији, 2025*. Београд: Републички завод за статистику.

Стратегија заштите података о личности за период од 2023. до 2030. године. „Службени гласник РС”, бр. 72/2023.

Устав Републике Србије. „Службени гласник РС”, бр. 98/2006 и 115/2021.

МЕНАЏЕРСКЕ КОМПЕТЕНЦИЈЕ У УСЛОВИМА ПРИМЕНЕ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ И ЗАШТИТЕ ПРИВАТНОСТИ

Саша Кукољ¹

Сажетак

Савремено пословно окружење обележено је убрзаном дигитализацијом и све интензивнијом применом вештачке интелигенције у различитим организационим и менаџерским процесима. Такве промене утичу на трансформацију традиционалне улоге менаџера и стварају потребу за развојем нових компетенција које обухватају технолошка, когнитивна, социјална и етичка знања и способности. Циљ овог рада је да се анализирају менаџерске компетенције у условима примене вештачке интелигенције, са посебним освртом на заштиту приватности, етичку одговорност и управљање ризицима. У раду су размотрени значај технолошке компетентности и писмености у области ВИ, одлучивања заснованог на подацима, емоционалне интелигенције, стратешког размишљања, комуникације, сарадње, адаптивности и управљања променама. Посебна пажња посвећена је трансформацији менаџерске улоге у условима у којима системи вештачке интелигенције преузимају део аналитичких, координационих и контролних активности. Анализа указује да улога менаџера не нестаје, већ се мења у правцу тумачења алгоритамских резултата, координације односа између људи и интелигентних система и обезбеђивања одговорности у процесу доношења одлука. Посебан изазов представља усклађивање захтева за транспарентношћу и објашњивошћу алгоритамских система са потребом за заштитом приватности и осетљивих података. Закључује се да успешна и одговорна примена вештачке интелигенције захтева интегрисан развој менаџерских компетенција, континуирано учење, људски надзор и јасно дефинисане механизме етичке и организационе одговорности.

Кључне речи: менаџерске компетенције, вештачка интелигенција, приватност, етичка одговорност, писменост у области ВИ, управљање ризицима.

¹ Факултет за менаџмент, Сремски Карловци –
Универзитет „Унион-Никола Тесла”, Београд, Србија
e-mail: sasa.kukolj@famns.edu.rs

УВОД

Вештачка интелигенција (ВИ) последњих година постаје све значајнији чинилац трансформације савремених организација, при чему њена примена више није ограничена само на аутоматизацију појединих техничких и оперативних активности. Системи засновани на вештачкој интелигенцији све чешће се укључују у процесе анализе података, доношења одлука, координације, контроле и управљања различитим организационим процесима. На тај начин мењају се традиционални односи између технологије, запослених и менаџмента, али и сама улога менаџера у организацији. Примена вештачке интелигенције стога не представља искључиво технолошко питање, већ и значајан организациони и управљачки изазов (Benlian et al., 2022; Santiago-Torner et al., 2026). У таквом пословном окружењу посебан значај добијају компетенције менаџера које треба да омогуће разумевање могућности и ограничења вештачке интелигенције, њено адекватно укључивање у пословне процесе и доношење одговорних одлука. Истраживања указују на то да компетенције неопходне за примену вештачке интелигенције не обухватају само техничка знања, већ и низ других способности, као што су критичко мишљење, прилагодљивост, комуникација, доношење одлука, емоционална интелигенција, управљање променама и континуирано учење. Посебно је значајно да се техничке и нетехничке компетенције развијају паралелно, јер се у пракси међусобно допуњују (Myszak & Filina-Dawidowicz, 2025).

Потреба за развојем нових компетенција произлази и из чињенице да вештачка интелигенција мења начин на који се послови обављају и како се доносе одлуке. У раду Santana и Díaz-Fernández (2023) показано је да један од значајних изазова за организације представља обезбеђивање радне снаге која поседује одговарајуће дигиталне компетенције, као и прилагођавање пракси управљања људским ресурсима (енгл. Human Resources, HR) новим условима примене вештачке интелигенције. Слично томе, Asemota (2026) закључује да промене у систему компетенција превазилазе искључиво техничке вештине и све више обухватају комбинацију техничког разумевања, менаџерског расуђивања, способности учења, управљачких способности и психолошке спремности за рад у окружењу у којем су људи и вештачка интелигенција међусобно повезани.

Развој компетенција посебно је значајан на нивоу руководиоца, јер успех примене вештачке интелигенције у великој мери зависи од начина на који менаџери разумеју и усмеравају њену употребу. Peifer и Terstegen (2024) указују да вештачка интелигенција може да подржи руководиоце у обављању лидерских задатака, као и да делимично преузме административне, координационе и контролне активности. Због тога је неопходно прилагођавати постојеће процесе, развијати одговарајуће програме квалификација и омогућити руководиоцима стицање компетенција потребних за увођење и употребу система вештачке интелигенције на начин који је оријентисан ка човеку (Peifer & Terstegen, 2024).

Истовремено, примена вештачке интелигенције отвара бројна питања која превазилазе ефикасност и пословне перформансе. Посебно су изражени изазови који се односе на одговорност, транспарентност, правичност, приватност и очување људске контроле над одлукама. Систематски преглед Sacavém et al. (2026) показује да се трансформација лидерства под утицајем вештачке интелигенције може посматрати кроз три међусобно повезане димензије: доношење одлука уз подршку вештачке интелигенције, промену лидерских компетенција и улога, као и етичке изазове који укључују одговорност, транспарентност, правичност, приватност и људску аутономију. Заштита приватности у том контексту постаје једно од важних питања са којима се суочавају савремени менаџери. Keaney и Berthon (2025) указују на постојање

стратешке дилеме између потребе за транспарентношћу и објашњивошћу система вештачке интелигенције, с једне стране, и потребе за заштитом личних и осетљивих података, с друге стране. Поступци којима се повећава објашњивост алгоритамских одлука могу истовремено створити ризик од откривања осетљивих података или пословно значајних информација, због чега решавање овог проблема није само технички задатак, већ и питање стратешког управљања (Keaney & Berthon, 2025).

Управо због тога све већи значај има и управљање вештачком интелигенцијом на организационом нивоу. Mäntymäki et al. (2022) наглашавају да је управљање вештачком интелигенцијом неопходно како би организације могле да користе њене предности, а истовремено контролишу ризике који се односе на пристрасност, дискриминацију, непрозирност и слабљење људске одговорности. Birkstedt et al. (2023) додатно указују да организационо управљање вештачком интелигенцијом обухвата правила, праксе и процесе којима се обезбеђује усклађеност њене употребе са стратегијом, циљевима, вредностима, законским захтевима и етичким принципима организације, при чему су посебно значајни обука, свест запослених, управљање заинтересованим странама, организациона култура и посвећеност највишег менаџмента.

Полазећи од наведеног, предмет овог рада јесу менаџерске компетенције у условима све шире примене вештачке интелигенције, са посебним освртом на питања приватности, етичке одговорности и управљања ризицима. Циљ рада је да се, на основу релевантне научне литературе, сагледају промене које вештачка интелигенција доноси у савременој менаџерској пракси, идентификују компетенције које су менаџерима потребне за њену одговорну примену и укаже на значај заштите приватности и успостављања одговарајућих механизма управљања вештачком интелигенцијом. Рад се састоји од шест делова. Након уводних разматрања, у другом делу разматране су менаџерске компетенције у савременом пословном окружењу, док се у трећем анализира примена вештачке интелигенције у менаџерској пракси. Четврти део посвећен је трансформацији менаџерских компетенција под утицајем вештачке интелигенције, а пети питањима заштите приватности и етичке одговорности менаџера. У шестом делу изложена су закључна разматрања рада.

МЕНАЏЕРСКЕ КОМПЕТЕНЦИЈЕ У САВРЕМЕНОМ ПОСЛОВНОМ ОКРУЖЕЊУ

Савремено пословно окружење карактеришу интензивна дигитализација, убрзане технолошке промене и све веће ослањање организација на податке и дигиталне технологије у процесима планирања, одлучивања и управљања. Такве промене непосредно утичу на начин обављања менаџерских активности и захтевају континуирано прилагођавање знања и способности руководиоца. Развој аутоматизације, машинског учења, роботике и, у новије време, генеративне вештачке интелигенције мења садржај послова, процесе доношења одлука и интеракцију између људи и технологије. Због тога се и компетенције све мање могу посматрати као статичан скуп знања и способности стечених у једном тренутку, а све више као динамичка категорија која се развија у складу са променама пословних процеса и технологије (Asemota, 2026). Промене у пословном окружењу не подразумевају да техничке компетенције у потпуности потискују традиционалне менаџерске и интерперсоналне способности. Напротив, савремени модели компетенција све више наглашавају њихово међусобно повезивање. Asemota

(2026) указује да се профил компетенција у окружењу заснованом на вештачкој интелигенцији помера од изолованих техничких вештина ка хибридным и портфолио конфигурацијама које повезују техничко разумевање, менаџерско расуђивање, способност учења и прилагођавања, управљачке способности и психолошку спремност. То значи да успешност менаџера све мање зависи од једне издвојене вештине, а све више од начина на који се различите компетенције комбинују и примењују у конкретној организационој ситуацији (Asemota, 2026).

Сличан приступ заступају Myszak и Filina-Dawidowicz (2025), који су систематизацијом релевантне литературе идентификовали 15 компетенција и вештина значајних за савремене лидере. Аутори их разврставају на тврде, меке и вишедимензионалне компетенције, истичући при томе да границе између појединих категорија нису увек оштре. Међу најчешће помињаним компетенцијама издвајају се технолошка компетентност и писменост у области вештачке интелигенције, емоционална интелигенција и одлучивање засновано на подацима. Истовремено, већина идентификованих компетенција припада групи меких компетенција, што показује да дигитализација не умањује значај способности управљања људима, комуникације и међуљудских односа (Myszak & Filina-Dawidowicz, 2025).

Одлучивање засновано на подацима представља једну од важних компетенција савременог менаџера. Оно подразумева доношење одлука заснованих на чињеницама, анализи и информацијама добијеним обрадом великих и сложених количина података, али без елиминисања људског расуђивања и пословног контекста. Другим речима, расположивост података сама по себи није довољна. Од менаџера се очекује способност њиховог тумачења и повезивања са конкретном пословном ситуацијом, организационим циљевима и последицама одлуке (Myszak & Filina-Dawidowicz, 2025).

Поред аналитичких способности, све већи значај има технолошка компетентност. Она не подразумева да менаџер мора бити програмер или стручњак за развој алгоритама. Важније је да поседује довољно знања да разуме основне принципе функционисања савремених технологија, њихове могућности, ограничења, користи и ризике. Myszak и Filina-Dawidowicz (2025) технолошку компетентност и писменост у области ВИ повезују не само са практичним коришћењем технологија већ и са разумевањем кључних концепата, алгоритама и начина на који системи вештачке интелигенције функционишу.

Benlian и Pinski (2025) додатно указују да писменост у области вештачке интелигенције има концептуалну, етичку и практичну димензију. Ниво и садржај такве компетенције зависе од положаја запосленог у организацији. Од највишег руководства очекује се пре свега разумевање стратешких могућности, ограничења и ризика, док средњи менаџери морају бити способни да високе стратешке циљеве претворе у оперативне процесе, интегришу технологију у свакодневни рад и воде тимове кроз промене (Benlian & Pinski, 2025). Ова разлика показује да савремене компетенције морају бити прилагођене конкретним менаџерским улогама и одговорностима.

Међутим, технолошко знање и аналитичке способности нису довољни за успешно управљање. Емоционална интелигенција задржава значајну улогу јер менаџер мора бити способан да препозна и управља сопственим емоцијама, разуме реакције сарадника, подржи тимску кохезију и обезбеди да процес промена остане усмерен ка људима. Myszak и Filina-Dawidowicz (2025) повезују емоционалну интелигенцију са самосвешћу, саморегулацијом, мотивацијом, емпатијом и социјалним способностима, наглашавајући њен значај за одговорно лидерство усмерено ка људима.

Значај комуникације, сарадње и прилагодљивости такође расте у условима брзих промена. Развој нових технологија захтева континуирано учење и способност прилагођавања новим ситуацијама, док успешна примена промена зависи од тога да ли менаџер може да комуницира

њихову сврху, укључи запослене и подстакне сарадњу. Анализа Myszak и Filina-Dawidowicz (2025) показује да су комуникација, сарадња, критичко размишљање, управљање променама, стратешко размишљање, адаптивна агилност и способност мотивисања и менторског усмеравања других саставни делови савременог лидерског профила.

Посебно је важно да се наведене компетенције не развијају изоловано. Одлучивање засновано на подацима може бити делотворније када је праћено емоционалном интелигенцијом и организационом агилношћу, док технолошка стручност добија пун ефекат тек када је повезана са сарадњом и способношћу управљања променама. На сличан начин, комуникација се повезује са креативношћу, а критичко размишљање са способношћу процене и тумачења сложених ситуација. Зато савремени профил менаџера треба посматрати као интегрисану целину међусобно повезаних компетенција, а не као списак независних способности (Myszak & Filina-Dawidowicz, 2025).

У табели 1, основна класификација тврдых, меких и вишедимензионалних компетенција непосредно је подржана налазима Myszak & Filina-Dawidowicz (2025). Хибридни карактер савременог профила компетенција потврђује Asemota (2026). Разлике у захтевима за писменост у области ВИ између руководилачких нивоа потврђују Benlian и Pinski (2025). Етичка одговорност, транспарентност, правичност и људски надзор као саставни део савременог лидерства подржани су и систематским прегледом Sacavém et al. (2026).

Табела 1. Кључне менаџерске компетенције у савременом пословном окружењу

Менаџерска компетенција	Садржај компетенције	Значај за савремену менаџерску праксу	Извор
Технолошка компетентност и писменост у области ВИ	Разумевање основних принципа, могућности, ограничења, користи и ризика савремених технологија и вештачке интелигенције.	Омогућава менаџеру да процени могућности примене технологије и да је повеже са пословним процесима и циљевима организације.	Myszak & Filina-Dawidowicz (2025); Benlian & Pinski (2025)
Одлучивање засновано на подацима	Коришћење чињеница, анализа и података при доношењу одлука уз задржавање људског расуђивања и уважавање пословног контекста.	Омогућава аргументованије одлучивање и коришћење аналитичких резултата у менаџерској пракси.	Myszak & Filina-Dawidowicz (2025)
Емоционална интелигенција	Самосвест, саморегулација, мотивација, емпатија и социјалне способности.	Доприноси вођењу људи, тимској кохезији и задржавању приступа усмереног ка човеку у условима технолошких промена.	Myszak & Filina-Dawidowicz (2025)

Стратешко размишљање и визија	Способност дефинисања будућег правца и повезивања технологије са дугорочним циљевима и вредностима организације.	Омогућава да технолошке иницијативе буду усклађене са стратегијом и приоритетима организације.	Myszak & Filina-Daw- idowicz (2025)
Комуникација и сарадња	Размена информација, повезивање различитих учесника и изградња сарадње и поверења.	Значајне су за прихватање промена, координацију тимова и повезивање техничких и пословних функција.	Myszak & Filina-Daw- idowicz (2025)
Адаптивна агилност и континуирано учење	Флексибилност, прилагођавање новим технологијама и ситуацијама, учење и промена стратегија у складу са новим околностима.	Омогућава менаџеру да одговори на динамичне технолошке и организационе промене.	Myszak & Filina-Daw- idowicz (2025); Asemo- ta (2026)
Управљање променама	Комбиновање планирања процеса и технологије са управљањем људима и њиховим реакцијама на промене.	Олакшава увођење нових технологија и њихову интеграцију у постојеће пословне процесе.	Myszak & Filina-Daw- idowicz (2025); Benlian & Pinski (2025)
Етичко лидерство и управљачка одговорност	Етичко расуђивање, разумевање ризика, одговорности, правичности, транспарентности и заштите приватности.	Омогућава да примена нових технологија буде усклађена са организационим вредностима и захтевима одговорног управљања.	Myszak & Filina-Daw- idowicz (2025); Asemo- ta (2026); Sacavém et al. (2026)

Извор: Систематизација аутора на основу Myszak и Filina-Dawidowicz (2025); Asemota (2026); Benlian, Pinski (2025); Sacavém et al. (2026).

На основу приказаног у табели 1 може се закључити да менаџерске компетенције у савременом пословном окружењу имају изразито комбинован карактер. Техничко и аналитичко знање мора бити повезано са стратешким размишљањем, способношћу комуникације и сарадње, емоционалном интелигенцијом, прилагодљивошћу и етичком одговорношћу. Посебно је значајно што Asemota (2026) компетенције више не посматра као фиксне и независне способности, већ као динамички портфолио који се мења у зависности од задатка, организационог дизајна и односа између човека и технологије. Овакав приступ представља добру основу за разматрање начина на који примена вештачке интелигенције додатно мења захтеве који се постављају пред савремене менаџере, што ће бити предмет наредних делова рада.

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА У САВРЕМЕНОЈ МЕНАѢРСКОЈ ПРАКСИ

Вештачка интелигенција све више постаје саставни део савремене менаџерске праксе, јер се њена примена шири са појединачних техничких задатака на активности које су традиционално припадале домену менаџмента. Алгоритамски системи данас могу да обављају анализу података, учествују у запошљавању и процени запослених, дају повратне информације о учинку, подржавају координацију и контролу, као и да доприносе доношењу сложенијих пословних одлука. Због тога вештачку интелигенцију није оправдано посматрати само као помоћно средство, већ као технологију која постепено мења начин на који се поједине менаџерске функције извршавају (Benlian et al., 2022).

Једна од најзначајнијих области примене вештачке интелигенције у менаџменту односи се на процес доношења одлука. Системи вештачке интелигенције омогућавају обраду великих количина података, уочавање образаца и брже генерисање информација које могу бити значајне за менаџерске одлуке. Систематски преглед Sacavém et al. (2026) показује да вештачка интелигенција може да убрза и прошири циклусе доношења одлука, али да тиме истовремено мења улогу менаџера. Његов задатак се постепено помера са непосредне аналитичке обраде података ка тумачењу резултата, координацији, постављању граница аутономије система и доношењу коначног суда у ситуацијама у којима алгоритамска препорука није довољна сама по себи (Sacavém et al., 2026).

Таква промена може се описати као прелазак менаџера од улоге класичног аналитичара ка улози „архитекте одлучивања”. У том моделу менаџер одређује на који начин ће бити подељени задаци између људи и система вештачке интелигенције, колики степен аутономије ће бити додељен алгоритму и у којим ситуацијама је неопходна људска интервенција. Sacavém et al. (2026) истичу да се лидерска улога све више повезује са пројектовањем односа човек–ВИ, институционализацијом надзора и очувањем одговорности за одлуке. Истовремено, менаџери се померају од искључиво хијерархијске контроле ка координацији различитих актера и функција које учествују у примени ВИ (Sacavém et al., 2026).

Примена вештачке интелигенције видљива је и у управљању људским ресурсима. Asemota (2026) указује на све израженије присуство ВИ у активностима као што су регрутовање, управљање учинком, учење и развој запослених и анализа радне снаге. Оваква примена не мења само начин извршавања појединачних HR активности, већ и компетенције које су потребне запосленима и менаџерима. Посебно се повећава значај способности сарадње између људи и интелигентних система, као и менаџерског расуђивања при процени резултата које генеришу

алгоритми (Asemota, 2026). Алгоритамски менаџмент представља посебно изражен облик овакве трансформације. Benlian et al. (2022) га описују као примену алгоритама који на основу података преузимају или подржавају послове координације, контроле и других традиционалних менаџерских активности. У пракси се то може односити на распоређивање послова, праћење учинка, оцењивање резултата и аутоматизовано давање повратних информација. Предност оваквог приступа огледа се у могућности обраде великог броја података и извршавању одређених менаџерских активности у великом обиму, али са растом аутономије система расту и питања транспарентности, контроле и разумљивости алгоритамских одлука (Benlian et al., 2022).

Примена ВИ такође може да промени природу комуникације и лидерства у организацијама. Када алгоритамски системи преузимају рутинске аналитичке и контролне активности, већи значај добијају они делови менаџерског рада који су усмерени на људе. Sacavém et al. (2026) наводе да комуникација, изградња поверења, емоционална интелигенција, менторство и подршка запосленима постају нарочито значајни када ВИ преузима део рутинских аналитичких послова. Истовремено, менаџери имају задатак да смање отпор према новим технологијама, објасне сврху њихове примене и развијају организациону културу у којој се ВИ користи на одговоран начин.

Вештачка интелигенција се, дакле, не примењује само ради аутоматизације, већ и ради подршке сложенијим менаџерским активностима. Међутим, њена већа употреба истовремено доводи до потребе за јаснијим дефинисањем одговорности. Osadchyi et al. (2026) указују да организациони лидери остају одговорни за исходе одлука заснованих на ВИ чак и када су сами системи сложени или непрозирни. Ако није јасно ко има овлашћење да надзире, заустави или коригује систем, долази до распршивања одговорности и повећања организационих ризика. Зато аутори управљање ВИ посматрају као менаџерску способност која обухвата расподелу овлашћења, дизајн одговорности, спремност на интервенцију и јасну комуникацију (Osadchyi et al., 2026).

Поред организационе ефикасности, примена ВИ у менаџменту мора се сагледавати и са становишта одговорног управљања. Алгоритамска пристрасност, нарушавање приватности и нејасна одговорност могу створити ризике и за организацију и за појединце. Arif et al. (2026) указују да одговорна примена ВИ захтева формалне механизме као што су процена ризика, надзорне структуре, механизми одговорности за учинак и континуирана евалуација. Значај има и опредељеност највишег менаџмента, која се испољава кроз комуникацију, формулисање политика и обезбеђивање потребних ресурса (Arif et al., 2026).

Табела 2. Основне области примене вештачке интелигенције у савременој менаџерској пракси

Област примене	Улога ВИ у менаџерској пракси	Извор
Доношење одлука	Обрада података, убрзавање анализе и подршка менаџерским одлукама, уз потребу за људским расуђивањем и надзором.	Sacavém et al. (2026); Myszak & Filina-Dawidowicz (2025)
Координација и контрола	Алгоритми могу делимично преузимати распоређивање, координацију, контролу и праћење учинка.	Benlian et al. (2022)
Управљање људским ресурсима	Примена у регрутовању, управљању учинком, учењу и развоју и анализи радне снаге.	Asemota (2026)

Лидерство и управљање променама	ВИ мења улогу менаџера ка координацији, тумачењу резултата, комуникацији, изградњи поверења и подршци запосленима.	Sacavém et al. (2026)
Управљање и надзор ВИ	Дефинисање одговорности, овлашћења, механизма интервенције, надзора и контроле ризика.	Osadchyi et al. (2026); Arif et al. (2026)

Извор: Систематизација аутора на основу Benlian et al. (2022); Myszak и Filina-Dawidowicz (2025); Asemota (2026); Sacavém et al. (2026); Arif et al. (2026); Osadchyi et al. (2026)

На основу наведеног у табели 2 може се уочити да увођење вештачке интелигенције не води једноставном нестанку менаџерске улоге, већ њеној трансформацији. Одређени аналитички, административни и контролни задаци могу бити делимично аутоматизовани, док се људска улога све више усмерава на тумачење, стратегијско усмеравање, координацију, процену ризика и очување одговорности.

Sacavém et al. (2026) ову промену описују као померање од рутинске анализе ка вишем нивоу расуђивања, координације и лидерства усмереног ка човеку. Управо због такве трансформације, питање више није само да ли ће менаџери користити вештачку интелигенцију, већ које компетенције морају развити да би је користили ефикасно, одговорно и у складу са организационим циљевима, што представља основу за наредно поглавље о трансформацији менаџерских компетенција у условима примене ВИ.

ТРАНСФОРМАЦИЈА МЕНАѢРСКИХ КОМПЕТЕНЦИЈА У УСЛОВИМА ПРИМЕНЕ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ

Примена вештачке интелигенције не мења само поједине менаџерске активности, већ постепено трансформише и сам профил компетенција које су потребне савременим руководиоцима. Ранији приступи су често посматрали компетенције као релативно стабилан скуп знања и вештина, док новија истраживања указују да се у окружењу заснованом на ВИ оне све више развијају као динамичне и међусобно повезане способности. Asemota (2026) истиче да се савремени профили померају од изолованих техничких вештина ка хибридним комбинацијама које обухватају техничко разумевање, менаџерско расуђивање, способност учења, управљачке компетенције и психолошку спремност за рад у окружењу у којем су људи и интелигентни системи међусобно повезани.

Посебно значајну промену представља раст значаја технолошке компетентности и писмености у области вештачке интелигенције. Од менаџера се не очекује да постану програмери, али морају да разумеју основне принципе функционисања ВИ, њене могућности,

ограничења и ризике. Myszak и Filina-Dawidowicz (2025) управо технолошку компетентност и писменост у области ВИ, заједно са одлучивањем заснованим на подацима и емоционалном интелигенцијом, издвајају као најчешће препознате компетенције лидера у анализираној литератури.

Истовремено, трансформација менаџерских компетенција не води ка смањењу значаја такозваних меких вештина. Напротив, њихов значај у појединим ситуацијама постаје још већи. Myszak и Filina-Dawidowicz (2025) показују да су емоционална интелигенција, комуникација, сарадња, стратешко размишљање, људско расуђивање, креативност, адаптивна агилност и способност мотивисања и менторског усмеравања запослених важан део лидерског профила. Аутори при томе наглашавају да је већина идентификованих компетенција управо из домена меких вештина, што потврђује да технолошка трансформација не умањује значај управљања људима. Промене су посебно видљиве у области доношења одлука. Како ВИ све више преузима анализу података и генерисање препорука, улога менаџера се помера ка процени, тумачењу и надзору алгоритамских резултата. Sacavém et al. (2026) указују да лидери у окружењу ВИ постепено прелазе из улоге класичних аналитичара у улогу „архитеката одлучивања”, који дефинишу поделу задатака између људи и система, границе аутономије и механизме надзора. На тај начин људско расуђивање не нестаје, већ добија нову улогу у контроли и усмеравању алгоритамски подржаних процеса.

Важан елемент трансформације представља и све већи значај етичких и управљачких компетенција. Asemota (2026) указује да савремени модели компетенција морају да укључе способности повезане са надзором ВИ, ублажавањем пристрасности, транспарентношћу, одговорношћу и сарадњом са стручњацима који развијају и примењују алгоритамске системе. Слично томе, Osadchyi et al. (2026) управљање вештачком интелигенцијом посматрају као посебну менаџерску способност засновану на расподели овлашћења, јасном дефинисању одговорности, спремности на интервенцију и организационој комуникацији. Посебну пажњу захтева континуирани развој компетенција. Benlian и Pinski (2025) истичу да се потребе за писменошћу у области ВИ разликују према организационом нивоу. Највиши менаџмент треба да развија стратешко разумевање ВИ, способност процене ризика и успостављања механизма одговорног управљања, док средњи менаџери морају више да се усмере на оперативну интеграцију, вођење тимова и примену ВИ у свакодневним процесима. Због тога развој компетенција треба да буде континуиран и прилагођен конкретним улогама и одговорностима.

На основу наведеног може се закључити да примена вештачке интелигенције не доводи до једноставне замене традиционалних менаџерских компетенција новим техничким знањима. Уместо тога, долази до њиховог проширивања, повезивања и преобликовања. Савремени менаџер мора истовремено да разуме технологију, доноси одлуке на основу података, управља људима и променама, примењује критичко и етичко расуђивање и обезбеђује да употреба ВИ остане под одговарајућим људским надзором. Управо ова комбинација техничких, когнитивних, социјалних и етичких компетенција представља основ савременог менаџерског профила у условима све шире примене вештачке интелигенције.

ЗАШТИТА ПРИВАТНОСТИ И ЕТИЧКА ОДГОВОРНОСТ МЕНАѢРА У ПРИМЕНИ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ

Све интензивнија примена вештачке интелигенције у пословним процесима доноси организацијама значајне користи, али истовремено отвара бројна питања у вези са приватношћу, правичношћу, транспарентношћу и одговорношћу. Због тога одговорна примена ВИ не може бити посматрана само као техничко питање које је у надлежности ИТ стручњака. Одлуке о томе које ће технологије бити примењене, које податке ће користити, у којим пословним процесима ће се примењивати и колики степен аутономије ће им бити дозвољен представљају и значајна менаџерска питања. Batool et al. (2025) наглашавају да етичка и одговорна вештачка интелигенција подразумева правичност, одговорност, транспарентност и инклузивност, при чему се посебна пажња мора посветити спречавању дискриминације, нарушавања приватности и угрожавања људског достојанства.

Заштита приватности је посебно значајна зато што савремени системи вештачке интелигенције у великој мери зависе од података. Управљање подацима због тога представља један од кључних елемената управљања ВИ на нивоу организације. Birkstedt et al. (2023) истичу да питања приватности, правне заштите и интегритета података представљају саставни део практичног управљања вештачком интелигенцијом. Истовремено, непрозирност алгоритама и немогућност да се у потпуности разуме начин на који систем долази до одређеног резултата додатно отежавају утврђивање одговорности и процену последица његове примене.

За менаџере се при томе јавља специфична дилема између транспарентности и приватности. С једне стране, алгоритамске одлуке треба да буду довољно објашњиве како би се могле контролисати и како би корисници и друге заинтересоване стране имали поверење у њих. С друге стране, повећање објашњивости може довести до откривања осетљивих података, пословних информација или карактеристика самог модела. Keaney и Berthon (2025) зато наглашавају да балансирање између објашњивости и приватности представља стратешки менаџерски проблем, а не само технички задатак. Од менаџера се очекује да разуме основне ризике и да успостави политике које истовремено подржавају транспарентност и заштиту података.

Етичка одговорност менаџера огледа се и у обезбеђивању одговарајућих механизма управљања и надзора. Batool et al. (2025) показују да управљање ВИ треба да одговори на питања ко је одговоран, шта се контролише, у којој фази животног циклуса система се контрола спроводи и на који начин се управљање реализује кроз правила, политике, алате и моделе. Посебан проблем представља чињеница да постојећи модели управљања не обухватају увек подједнако све етичке принципе. Анализа истих аутора показује да поједина решења недовољно обухватају питања правичности, транспарентности, приватности и поверења, због чега је потребан систематичнији и свеобухватнији приступ управљању ризицима ВИ (Batool et al., 2025). Одговорна примена, међутим, не може бити обезбеђена само формалним правилима и техничким механизмима. Sturm et al. (2026) указују на значај међусобног деловања организационих структура и људског расуђивања. Према њиховом приступу, правила, процедуре и технолошки алати стварају оквир за одговорну употребу ВИ, али запослени и руководиоци морају бити способни да процене како та правила треба применити у конкретној ситуацији. Одговорно управљање ВИ стога представља континуирану организациону праксу у којој се формални механизми и људско расуђивање међусобно допуњују (Sturm et al., 2026).

Овакав приступ посебно наглашава значај менаџерске процене. Sturm et al. (2026), на примеру организационе примене ВИ, показују да ниједан појединачни механизам управљања није довољан сам за себе. Смернице за одговорну примену, анализа последица и обуке за-

послених могу да усмере понашање, али у реалним пословним ситуацијама остаје потреба за људским расуђивањем и способношћу прилагођавања правила конкретним околностима. То значи да етичка компетенција менаџера није ограничена на познавање правила, већ подразумева и способност препознавања ситуација у којима формално прописана процедура није довољна за доношење одговорне одлуке.

Практична етичка одговорност подразумева и успостављање механизма сталног надзора. Birkstedt et al. (2023) међу основним организационим механизмима управљања ВИ издвајају надзор, ревизију и процену ризика и утицаја, уз различите облике задржавања човека у процесу одлучивања. Такви механизми су значајни јер менаџерска одговорност не престаје у тренутку када се систем ВИ уведе у употребу. Потребно је континуирано процењивати његове резултате, могуће пристрасности и последице по кориснике, запослене и друге заинтересоване стране.

Посебан значај има и развој организационе културе одговорне употребе ВИ. Етичко поступање не може зависити искључиво од личне иницијативе појединачних запослених, већ мора бити подржано обукама, процедурама и јасном посвећеношћу руководства. Arif et al. (2026) истичу да обуке из области етике ВИ могу допринети развоју знања и способности потребних за препознавање алгоритаМСких ризика, тумачење резултата и примену етичких принципа приликом доношења одлука. Истовремено, посвећеност руководства огледа се у комуникацији, развоју политика и обезбеђивању ресурса за одговорну примену ВИ.

На основу наведеног може се закључити да заштита приватности и етичка одговорност представљају саставни део савремених менаџерских компетенција. Од менаџера се очекује да разуме ризике који произлазе из употребе података, обезбеди одговарајући ниво транспарентности, јасно дефинише одговорност, успостави механизме људског надзора и обезбеди да организациона примена ВИ остане у складу са основним етичким вредностима. При томе формална правила и техничке мере нису довољне без способности менаџера и запослених да их правилно тумаче и примењују у конкретним околностима. Управо спој технолошког разумевања, етичког расуђивања, заштите приватности и организационе одговорности представља један од најзначајнијих захтева који примена вештачке интелигенције поставља пред савременог менаџера.

ЗАКЉУЧАК

Примена вештачке интелигенције значајно мења савремено пословно окружење и поставља нове захтеве пред менаџере. Поред традиционалних управљачких способности, све већи значај имају технолошка писменост, одлучивање засновано на подацима, критичко размишљање, прилагодљивост, емоционална интелигенција и способност управљања променама. Истовремено, развој ВИ повећава значај етичког расуђивања, људског надзора и јасног дефинисања одговорности у процесима доношења одлука. Посебан изазов представља заштита приватности и одговорно коришћење података. Савремени менаџер мора бити способан да усклади предности које ВИ доноси са захтевима транспарентности, правичности, безбедности и заштите личних података. Због тога се менаџерске компетенције у условима примене ВИ све више развијају као интегрисан скуп техничких, когнитивних, социјалних и етичких способности. Може се закључити да вештачка интелигенција не умањује значај менаџера, већ мења његову улогу. Уместо искључивог ослањања на контролу и рутинско одлучивање, савремени менаџер све више постаје координатор односа између људи и интелигентних система, тумач

алгоритамских резултата и носилац одговорности за њихову примену. Континуирани развој менаџерских компетенција зато представља један од кључних предуслова за ефикасну, етичку и одговорну примену вештачке интелигенције у организацијама.

РЕФЕРЕНЦЕ

Arif, M., Zhao, L., Zou, X., Li, K., Chen, Z., Ai, Y., & Tian, M. (2026). Ethics training competencies and leadership enable responsible AI in hospitality and tourism. *iScience*, 29(3). <https://doi.org/10.1016/j.isci.2026.115134>

Asemota, M. O. (2026). Artificial intelligence and the reconfiguration of competency management systems in organizations. *Discover Artificial Intelligence*, 6(1), 892. <https://doi.org/10.1007/s44163-026-02055-9>

Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: a systematic literature review. *AI and Ethics*, 5(3), 3265-3279. <https://doi.org/10.1007/s43681-024-00653-w>

Benlian, A., & Pinski, M. (2025). The AI literacy development canvas: Assessing and building AI literacy in organizations. *Business Horizons*. <https://doi.org/10.1016/j.bushor.2025.10.001>

Benlian, A., Wiener, M., Cram, W. A., Krasnova, H., Maedche, A., Möhlmann, M., Recker, J., & Remus, U. (2022). *Algorithmic management: bright and dark sides, practical implications, and research opportunities*. *Business & Information Systems Engineering*, 64 (6), 825–839. <https://doi.org/10.1007/s12599-022-00764-w>

Birkstedt, T., Minkinen, M., Tandon, A., & Mäntymäki, M. (2023). AI governance: themes, knowledge gaps and future agendas. *Internet Research*, 33(7), 133-167. <https://doi.org/10.1108/INTR-01-2022-0042>

Keaney, S., & Berthon, P. (2025). Balancing explainability and privacy in AI systems: A strategic imperative for managers. *Business Horizons*. <https://doi.org/10.1016/j.bushor.2025.10.004>

Mäntymäki, M., Minkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, 2(4), 603-609. <https://doi.org/10.1007/s43681-022-00143-x>

Myszak, J. M., & Filina-Dawidowicz, L. (2025). Leaders' competencies and skills in the era of artificial intelligence: A scoping review. *Applied Sciences*, 15(18), 10271. <https://doi.org/10.3390/app151810271>

Osadchyi, V., Shantyr, A., Zinchenko, O., Bondarchuk, A., Lashchevska, N., & Osadcha, K. (2026). Educating Managers to Govern Artificial Intelligence. *Sustainability*, 18(11), 5590. <https://doi.org/10.3390/su18115590>

Peifer, Y., & Terstegen, S. (2024). Artificial intelligence–qualification and competence development requirements for executives. *Procedia Computer Science*, 232, 736-744. <https://doi.org/10.1016/j.procs.2024.01.073>

Sacavém, A., Machado, A. D. B., Rodrigues dos Santos, J., Palma-Moreira, A., & Au-Yong-Oliveira, M. (2026). AI-driven leadership: decision-making, competencies, and ethical challenges-a systematic review. *Administrative Sciences*, 16(4), 173. <https://doi.org/10.3390/admsci16040173>

Santana, M., & Díaz-Fernández, M. (2023). Competencies for the artificial intelligence age: visualisation of the state of the art and future perspectives. *Review of Managerial Science*, 17(6), 1971-2004. <https://doi.org/10.1007/s11846-022-00613-w>

Santiago-Torner, C., Corral-Marfil, J. A., & Tarrats-Pons, E. (2026). Artificial intelligence and leadership in organizations: A PRISMA systematic review of challenges, risks, and governance dynamics. *Sustainability*, 18(8), 4085. <https://doi.org/10.3390/su18084085>

Sturm, S., Krause, F., & van Giffen, B. (2026). Beyond control? Governing AI in organizations for responsible use. *European Management Journal*. <https://doi.org/10.1016/j.emj.2026.06.003>

МЕДИЈСКА ПИСМЕНОСТ И СВЕСТИ ГРАЂАНА О ЗАШТИТИ ПРИВАТНОСТИ – РАЗЛИКЕ ИЗМЕЂУ ГЕНЕРАЦИЈА И НИВОА ОБРАЗОВАЊА

Драган Ђукановић¹

Сажетак

Рад анализира однос између медијске писмености и свести грађана о заштити приватности у Србији, са посебним освртом на генерацијске разлике и ниво образовања. Полазиште је схватање медијске писмености као скупа компетенција које обухватају приступ медијима, критичку процену садржаја, учешће у комуникацији, дигиталну безбедност и одговорно управљање личним подацима. Анализа је заснована на секундарној обради резултата више домаћих истраживања спроведених од 2022. до 2025. године, укључујући истраживања „Грађани и медији”, „Перцепција грађана о заштити података о личности”, истраживање медијских корисника старијих од 65 година, истраживање медијске писмености опште популације из 2025. и пилот студија „Интегрисани индекс медијске писмености Србије”. Налази показују да млађе генерације имају предност у техничким и платформским вештинама, али да дигитална спретност не гарантује критичку процену извора и садржаја. Старије генерације су изложеније дигиталном искључивању, посебно када се старост укрсти са нижим образовањем и животом у руралној средини. Ниво образовања се показује као један од најстабилнијих фактора који повезује шири избор извора, критичније читање медија, боље разумевање ризика и активније мере заштите приватности. Закључује се да јавне политике медијске писмености и заштите приватности треба да буду диференциране према старосним и образовним групама и усмерене на практичне компетенције, а не само на технички приступ дигиталним технологијама.

Кључне речи: медијска писменост, приватност, заштита података о личности, генерације, образовање, дигиталне компетенције, Србија.

¹ Драган Ђукановић, ТВ Мост Нови Сад, Србија,
e-mail: dragandjukadoco@gmail.com

УВОД

Савремено медијско окружење обележавају истовремено обиље информација, убрзана производња садржаја, растућа улога друштвених мрежа и алгоритамских препорука, све веће присуство садржаја генерисаних вештачком интелигенцијом и непрекидно прикупљање података о корисницима. У таквим условима, способност грађана да приступе медијима више није довољна да би се говорило о стварној медијској писмености. Кључно питање постаје на који начин грађани процењују веродостојност извора, препознају манипулативне форме, разумеју економску и технолошку логику платформи и штите сопствену приватност. Медијска и дигитална писменост све се више посматрају као повезане компетенције. У оквирима које користе UNESCO и европске институције, медијска писменост обухвата приступ, анализу, евалуацију, креирање и комуникацију садржаја, док савремени модели томе додају безбедност, управљање приватношћу и разумевање алгоритамски посредованог окружења. Пилот модел Интегрисаног индекса медијске писмености Србије експлицитно је укључио „поверење, приватност и сајбер-безбедност” као једну од шест димензија националног индекса, чиме је заштита приватности институционално повезана са медијском писменошћу (Матовић и др., 20256).

Питање приватности је у овом контексту двоструко. Са једне стране, грађани су корисници дигиталних медија који остављају личне податке, фотографије, локацијске трагове и податке о понашању. Са друге стране, они су субјекти медијског извештавања, па њихова приватност може бити угрожена објављивањем фотографија, здравствених података, података о породичном животу или других информација без оправданог јавног интереса. Кроз оба аспекта провлачи се и питање медијске писмености: колико грађани разумеју последице сопственог понашања, али и колико познају своја права када су предмет туђег објављивања.

Циљ овог рада је да, на основу доступних емпиријских истраживања у Србији, испита однос медијске писмености и свести о приватности, са посебним освртом на разлике између генерација и различитих нивоа образовања. Основна теза је да старост сама по себи не објашњава медијске компетенције. Генерацијска припадност пре свега усмерава избор медијског окружења и платформи, док ниво образовања значајно утиче на квалитет употребе, критичку процену, разноврсност извора и способност заштите личних података. Због тога се највеће разлике појављују тек када се старост укрсти са образовањем, дигиталним искуством и местом становања.

ПОЈАМ МЕДИЈСКЕ ПИСМЕНОСТИ У САВРЕМЕНОМ ДИГИТАЛНОМ ОКРУЖЕЊУ

Медијска писменост је током последњих деценија прошла од релативно уског појма разумевања масовних медија до сложеног скупа компетенција за живот у дигитализованом информационом окружењу. Европска комисија је медијску писменост везивала за способност приступа различитим медијима, разумевање начина њиховог функционисања и критичко вредновање садржаја. UNESCO медијску и информациону писменост дефинише као скуп знања, вештина, ставова и пракси који омогућавају приступ, анализу, критичку процену, тумачење, употребу, креирање и ширење информација и медијских производа на креативан, законит и етички начин (UNESCO, 2025).

У националном моделу развијеном за Србију задржане су три основне димензије које се појављују у већини савремених оквира: приступ и коришћење, критичка евалуација и партиципација. Међутим, аутори Интегрисаног индекса наглашавају да медијска писменост није атрибут појединца „у вакууму”, већ резултат односа индивидуалних компетенција и ширег окружења: квалитета образовања, доступности различитих извора, медијских слобода, демократских институција, инфраструктуре и механизма заштите корисника (Матовић и др., 2025б). Ово је важно јер једнако технички способни корисници могу имати веома различите могућности за критичко и безбедно коришћење медија. Такав приступ омогућава да се избегне честа грешка у јавном говору: изједначавање техничке вештине са медијском писменошћу. Брзина коришћења телефона, познавање апликација или присуство на већем броју друштвених мрежа јесу корисне дигиталне компетенције, али не гарантују способност утврђивања извора вести, разликовања чињенице од коментара, препознавања прикривеног оглашавања, провере фотографије или разумевања начина на који алгоритам бира садржај који ће кориснику бити приказан. Управо се у том раздвајању „техничког” и „критичког” налази кључ за разумевање генерацијских разлика. Истраживање медијске писмености опште популације Србије из 2025. године показује да је приступ медијима широк, али да су критичке праксе ограничене. Телевизију гледа 96,7% испитаника, друштвене мреже користи 57,5%, а платформе вештачке интелигенције 25,4%. Истовремено, 47,9% испитаника ретко или никада не проверава информације у више извора, 90,3% ретко или никада не користи сајтове за проверу чињеница, а 71,9% наводи да никада не препознаје садржај направљен уз помоћ вештачке интелигенције (Матовић и др., 2025а). Ово указује на јаз између приступа и квалитета употребе.

ПРИВАТНОСТ КАО САСТАВНИ ДЕО МЕДИЈСКЕ И ДИГИТАЛНЕ ПИСМЕНОСТИ

Право на приватност и заштиту података о личности има правну, етичку и практичну димензију. Закон о заштити података о личности Републике Србије уређује права физичких лица у вези са обрадом личних података, начела обраде, обавезе руковалаца и механизме правне заштите (Закон о заштити података о личности, 2018). За грађанина, међутим, формално постојање права не значи аутоматски и способност да то право препозна и оствари. Управо зато је свест о приватности део функционалне дигиталне писмености.

У дигиталном окружењу приватност подразумева способност управљања видљивошћу сопствених података, разумевање услова коришћења платформи, контролу локације, лозинки и дозвола апликација, препознавање покушаја преваре и процену последица дељења туђих фотографија и информација. Савремени концепт медијске писмености зато не може бити ограничен на питање „да ли је вест тачна”, већ обухвата и питање „које податке остављам, ко их види и са којом сврхом” (Матовић и др., 2025б).

Приватност има и медијску димензију која превазилази понашање самих корисника. Кодекс новинара и новинарки Србије у поглављу о поштовању и заштити приватности захтева од медија да штите идентитет жртава и других лица и да приватне податке и записе са друштвених мрежа не објављују без сагласности, осим када јавни интерес претеже над правом на приватност (Савет за штампу, 2025). Мониторинзи Савета за штампу и организација цивилног друштва показују да повреде приватности остају присутан проблем медијске праксе,

што значи да медијска писменост грађана мора укључити и познавање права према медијима, а не само правила безбедног понашања на интернету.

Истраживање „Перцепција грађана о заштити података о личности” из 2023. показало је да 80% грађана процењује ризик од злоупотребе личних података као висок, али истовремено већина сматра да грађани нису довољно упознати са својим правима. Посебно су важни налази да 75,5% сматра објављивање фотографија или видео-записа других лица на друштвеним мрежама без сагласности повредом података о личности и да 43,4% корисника интернета наводи да подешава приватност на друштвеним мрежама (Kantar Serbia & TMG Insights, 2023). Ово показује да декларативна свест о ризику постоји, али су практичне мере неравномерно распрострањене.

МЕТОДОЛОШКИ ПРИСТУП И ИЗВОРИ ПОДАТАКА

Овај рад има карактер прегледно-аналитичког истраживања. Не спроводи се ново примарно анкетирање, већ се примењује секундарна анализа резултата више релевантних истраживања која су у Србији мерила медијске навике, медијску и дигиталну писменост, свест о заштити података и специфичности старијих корисника. Основна предност оваквог приступа је могућност повезивања налаза који су у оригиналним студијама често анализирани одвојено. Истовремено, потребно је нагласити ограничење: студије нису спроведене на истим узорцима, не користе идентичне старосне категорије, нити у потпуности исте индикаторе. Истраживање „Грађани и медији” из 2022. обухвата испитанике од 12 до 60 година и користи генерацијске категорије, истраживање приватности из 2023. обухвата пунолетну популацију 18+, студија старијих медијских корисника фокусира се на 65+, док истраживање медијске писмености из 2025. обухвата грађане од 18 до 75 година. Зато се подаци користе за идентификовање образаца и односа, а не за механичко поређење свих процената.

Табела 1. Кључни извори коришћени у анализи

Извор: аутор, 2026.

Извор	Година	Узорак	Фокус
„Грађани и медији” (CeSID/Propulsion)	2022	1.199, узраст 12–60	медијске навике, медијска и дигитална писменост, приватност
„Перцепција грађана о заштити података о личности”	2023	1.211, 18+	свест о правима, ризицима и праксама заштите приватности
„Медијски корисници старији од 65 година у Србији”	2023	402, 65+	Традиционални и дигитални медији, образовање, дигитални јаз
„Медијска писменост грађана Србије”	2025	800, узраст 18–75	приступ, критичко читање, провера, партиципација, дигиталне вештине
„Индекс медијске писмености у Србији 2025”	2025/2026	индекс заснован на анкети и екстерним индикаторима	индивидуалне компетенције и фактори окружења

СТАЊЕ МЕДИЈСКЕ ПИСМЕНОСТИ У СРБИЈИ

Најновије репрезентативно истраживање медијске писмености опште популације спроведено је од 15. маја до 15. јуна 2025. на узорку од 800 испитаника старости од 18 до 75 година. Узорак је омогућавао анализу по старости, образовању, региону и типу насеља (Матовић и др., 2025a). Резултати показују да телевизија и даље има готово универзалан домет, док је употреба дигиталних медија широка, али неједнака. Важнији проблем од самог приступа представља ограничена навика критичке провере и пасивно коришћење медија.

Чак 68,6% грађана навело је да се свакодневно или често осећа преоптерећено информацијама и медијским садржајима, док 58,3% често или свакодневно наилази на медијске информације које изазивају снажне негативне емоције. У таквом окружењу провера садржаја је посебно важна, али скоро половина испитаника ретко или никада не проверава исту информацију у више извора. Још је упадљивији податак да 90,3% ретко или никада не користи специјализоване сајтове за проверу чињеница, док 89,7% истинитост информације проверава консултовањем са неким кога познаје (Матовић и др., 2025a).

Ови налази показују да неповерење у медије није исто што и медијска писменост. Грађанин може бити веома скептичан према телевизији, новинама или порталима, али да истовремено не располаже систематичном процедуром за проверу извора. Уместо институционалних или професионалних механизма провере, поверење се пребацује на личне мреже, што може ојачати ефекте информационих мехурова и друштвене хомогености.

Пилот Индекс медијске писмености за 2025. додатно је квантификовао овај проблем. Индекс заснован само на индивидуалним компетенцијама износи 35,9 од 100 поена. Чак 61% грађана налази се у категоријама ниског или веома ниског нивоа медијске писмености, док је само 7% у категорији високог нивоа, а нико у узорку није достигао категорију веома високог нивоа. Када се индивидуалним компетенцијама додају фактори окружења, Интегрисани индекс износи 43,11 од 100 и класификује се као средње-низак ниво (Матовић и др., 2025b).

За тему овог рада посебно је значајно што димензија „поверење, приватност и сајбер-безбедност” има скор 38,52, док је „припремљеност за вештачку интелигенцију” најнижа са 23,42. То значи да се проблем медијске писмености у Србији не може свести на доступност уређаја и интернета. Напротив, аутори индекса наглашавају велики раскорак између инфраструктурних могућности и начина на који их грађани стварно користе (Матовић и др., 2025b).

Табела 2. Одабрани показатељи медијске писмености у Србији, 2025.

Показатељ	Проценат/скор
Гледа телевизију	96,7%
Користи друштвене мреже	57,5%
Ретко или никада проверава информацију у више извора	47,9%
Ретко или никада користи сајтове за проверу чињеница	90,3%
Никада не препознаје садржај направљен уз помоћ ВИ	71,9%
ИМР – индивидуалне компетенције	35,9/100
ПМР – интегрисани индекс	43,11/100
Поверење, приватност и сајбер-безбедност	38,52/100

Извор: Матовић и др., 2025a, 2025b

СВЕСТ ГРАЂАНА О ЗАШТИТИ ПРИВАТНОСТИ

Истраживање из 2023. године показује занимљив спој високе забринутости и ограниченог познавања механизма заштите. Осам од десет грађана процењује ризик од злоупотребе личних података као висок, али истовремено преовлађује став да грађани нису довољно информисани о својим правима. Највећа потреба за додатним информацијама односи се на то ко сме да тражи личне податке, коме се грађанин може обратити у случају злоупотребе, која права има и шта све представља повреду података о личности (Kantar Serbia & TMG Insights, 2023).

Ово раздвајање забринутости и практичног знања важно је за концепт медијске писмености. Висока свест да „опасност постоји” не значи да корисник зна како да препозна ризик у конкретној ситуацији или да подеси систем заштите. У истраживању из 2023. 59,3% грађана наводи да податке не даје изворима које не сматра поузданим, 43,4% подешава приватност на друштвеним мрежама, а мањи удели користе друге специфичне мере. Извештај посебно указује да су старији, ниже образовани и становници села осетљивије групе и да су мање заинтересовани за тему заштите података (Kantar Serbia & TMG Insights, 2023).

Додатни аспект представља однос према приватности других. Три четвртине грађана препознаје да објављивање фотографија и снимака других лица на друштвеним мрежама без њихове сагласности представља повреду. Ово је значајан ниво нормативне свести, али се мора посматрати уз податак да велики број корисника на интернету редовно објављује сопствене и туђе фотографије. Разлика између познавања правила и понашања у свакодневном окружењу представља једну од централних тема практичне медијске писмености.

Када се приватност посматра у односу на професионалне медије, проблем добија додатну тежину. Савет за штампу је у мониторингу за другу половину 2025. навео да су међу најчешће кршеним поглављима Кодекса управо истинитост извештавања, поштовање и заштита приватности и одговорност новинара. То значи да грађанину нису потребне само компетенције самозаштите од платформи, већ и знање о томе када медиј прелази границу јавног интереса и како се може захтевати заштита (Савет за штампу, 2026).

ГЕНЕРАЦИЈСКЕ РАЗЛИКЕ У МЕДИЈСКИМ НАВИКАМА И КРИТИЧКИМ КОМПЕТЕНЦИЈАМА

Генерацијске разлике најпре се уочавају у избору канала информисања. Истраживање „Грађани и медији” из 2022. показује да су друштвене мреже и инфлуенсери значајнији за генерацију Z, док значај телевизије, радија и штампе расте са годинама. Међутим, подаци не подржавају поједностављен закључак да је најмлађа генерација уједно и медијски најписменија (Коматина, Раковић, & Јеремић, 2022).

На питању обраћања пажње на изворе медијских информација добија се посебно поучан резултат. Међу старијим припадницима генерације Z, од 19 до 26 година, збир оних који често или редовно обраћају пажњу на извор износи 29%, док је код млађих припадника генерације Z, од 12 до 18 година, само 11%. Код бејби бумера тај збир је 17% (Коматина и др., 2022). То значи да техничка блискост са дигиталним платформама није довољна за развој критичке

навике провере. Унутар саме генерације Z постоји, дакле, значајна разлика између адолесцената и млађих одраслих. Могуће објашњење лежи у развојном узрасту, нивоу образовања и већем искуству са сложенијим облицима информисања код групе 19–26. Ова група више користи портале, подкасте и различите дигиталне изворе, док најмлађи чешће бораве у окружењу кратких видео-формата и персонализованих друштвених мрежа. Зато би програми медијске писмености за адолесцените требало да буду усмерени на проверу извора, препознавање комерцијалног садржаја, алгоритамске препоруке и последице дељења личних података.

Код старијих генерација ризик је другачије природе. Традиционални медији, пре свега телевизија, имају већу улогу у информисању, а употреба интернета и дигиталних алата је мања. Међутим, старост не треба тумачити као јединствену категорију. Истраживање медијских корисника старијих од 65 година показало је да постоје огромне разлике унутар старе популације и да образовање, урбано или рурално место становања и материјални статус снажно мењају медијски профил (Матовић, Милин Перковић, & Јосифовић, 2023).

Табела 3. Одабране генерацијске разлике

Показатељ	Група	Резултат
Често или редовно обраћа пажњу на извор	Генерација Z, 12–18	11%
Често или редовно обраћа пажњу на извор	Генерација Z, 19–26	29%
Често или редовно обраћа пажњу на извор	Бејби бумери	17%
Зна како да заштити своје податке на интернету	Генерација Z, 19–26	73%
Зна како да заштити своје податке на интернету	Бејби бумери	26%

Извор: Коматина и др., 2022

НИВО ОБРАЗОВАЊА КАО ФАКТОР МЕДИЈСКЕ И ДИГИТАЛНЕ ПИСМЕНОСТИ

Док генерацијска припадност снажно утиче на избор медијских платформи, образовање се у доступним истраживањима показује као стабилан фактор квалитета употребе. Више образовање је повезано са чешћим коришћењем различитих извора, већом употребом интернет портала, бољим познавањем дигиталних система и већим бројем активних мера заштите приватности. Истраживање „Грађани и медији” наводи да су на широком скупу дигиталних компетенција изнад просека били запослени, становници урбаних средина и високообразовани испитаници, нарочито у старосној групи 19–41 година (Коматина и др., 2022).образовање не делује само кроз формално знање. Оно је повезано са већом изложеношћу различитим изворима, навиком читања сложенијих текстова, способношћу процене аргумената и вероватнијим коришћењем интернета у професионалне и информативне сврхе. Зато се не може рећи да диплома сама по себи „производи” медијску писменост, али она често представља индикатор ширег скупа когнитивних и социјалних ресурса који олакшавају критичко коришћење медија.

Истраживање приватности из 2023. такође издваја ниже образоване као једну од осетљивих група. Средње и високо образовани испитаници чешће препознају одговорност појединаца, државе и Повереника у систему заштите података и чешће користе активне стратегије избегавања непоузданих извора. Истовремено, занимљиво је да су испитаници са нижим образовањем понекад склонији уверењу да своје податке штите у довољној мери. То показује

да субјективна самопроцена не мора да буде једнака објективној разноврсности заштитних пракси (Kantar Serbia & TMG Insights, 2023).

Најјаснији пример значаја образовања налази се у популацији старијој од 65 година. У студији из 2023. интернет користи само 6,5% испитаника са основним или нижим образовањем, 62,19% са средњим и чак 85,9% са вишим или високим образовањем. Разлика између крајњих група већа је од 79 процентних поена (Матовић и др., 2023). Овај податак показује да „старост” није довољно објашњење дигиталног јаза; међу старијима образовање драматично мења вероватноћу учешћа у дигиталном медијском окружењу.

Табела 4. Употреба интернета међу старијима од 65 година према образовању

Ниво образовања	Користи интернет
Основно и ниже	6,5%
Средње	62,19%
Више и високо	85,9%

Извор: Матовић, Милин Перковић и Јосифовић, 2023

УКРШТАЊЕ ГЕНЕРАЦИЈЕ И ОБРАЗОВАЊА

Најважнији аналитички закључак овог рада произлази из укрштања старости и образовања. Генерација одређује вероватно медијско окружење у коме ће се грађанин кретати, док образовање значајно утиче на то како ће то окружење користити. Због тога су статистички и практично најрањивије комбинације оне у којима се генерацијски ризик удружује са ниским образовањем, ограниченим дигиталним искуством и слабијим социјалним ресурсима.

Млади са вишим нивоом образовања

Млађи одрасли са средњим и вишим образовањем имају најповољнију комбинацију техничке спретности, широког приступа платформама и развијенијих критичких навика. Група од 19 до 26 година у истраживању из 2022. издваја се по већем обраћању пажње на изворе и по познавању начина заштите личних података. Међутим, ни ова група није заштићена од ризика. Управо због интензивног коришћења друштвених мрежа, електронске трговине и различитих апликација, она оставља већу количину података и изложена је напреднијим облицима праћења, профилисања и манипулативног дизајна.

За ову групу медијска писменост мора да пређе са основних савета о „јакој лозинки” на напредније разумевање алгоритама, дигиталног профилисања, колачића, праћења понашања, вештачке интелигенције и пословних модела платформи. Другим речима, виши ниво техничких способности захтева и виши ниво медијско-информационог образовања.

Млади са нижим нивоом образовања

Код младих са нижим образовањем може се појавити специфичан облик дигиталне рањивости: висока учесталост коришћења телефона и друштвених мрежа уз слабије развијене критичке навике. Подаци о најмлађој генерацији Z показују да тек мали део редовно обраћа пажњу на извор. Ако се томе дода нижи образовни капитал, повећава се ризик да платформска вештина буде погрешно тумачена као компетентност за процену информација. Ова група захтева школске и ваншколске програме који су везани за конкретне платформе и свакодневне ситуације: препознавање спонзорисаног садржаја, процену кредибилитета инфлуенсера, проверу визуелних садржаја, последице јавног дељења фотографија и локације, као и права лица чије се фотографије или подаци објављују без сагласности. Такве компетенције треба развијати пре него што корисник постане правно и економски самосталан.

Средње генерације

Миленијалци и генерација X налазе се између две медијске логике. Одрасли су у окружењу телевизије, радија и штампе, али су професионални и приватни живот наставили у дигиталном окружењу. Овај „двоструки” медијски капитал може бити предност јер омогућава поређење традиционалних и дигиталних извора, али може стварати и информационо прептерећење. Истраживања показују да групе у активном радном добу имају широк приступ медијима, али то не значи да систематски користе алате за проверу чињеница.

Код средњих генерација ниво образовања постаје посебно важан јер утиче на избор извора и начин употребе интернета. Високообразовани чешће користе интернет портале, дигиталне услуге и разноврсне канале, док ниже образовани чешће задржавају ужи медијски репертоар. За приватност је значајно и то што су ове генерације најчешће економски активне, користе електронско банкарство, онлајн куповину и службене дигиталне системе, па су изложене и финансијски мотивисаним преварама и крађи идентитета.

Старији са вишим и високим образовањем

Старији високообразовани грађани најбоље показују зашто је опасно стереотипно изједначавати старост са дигиталном неписменашћу. У популацији 65+ чак 85,9% више и високо образованих користи интернет. Ова група може активно да прати портале, комуницира путем апликација и користи дигиталне услуге, а традиционални медији нису њен једини извор. Њен ризик произлази више из промене технолошких стандарда и нових облика преваре него из самог одсуства приступа. Програми намењени овој групи зато не би требало да буду патерналистички и сведени на „основе коришћења телефона”. Кориснији су модули о новим облицима преваре, провери извора, дипфејк садржају, управљању дозволама апликација и приватношћу у здравственим, банкарским и јавним дигиталним услугама. Истраживање старијих корисника препоручује и међугенерациску сарадњу у којој старији нису само примаоци знања већ и учесници који преносе искуство и критичке перспективе (Матовић и др., 2023).

Старији са нижим образовањем

Старији са основном школом или нижим образовањем представљају најизраженију зону дигиталног јаза. Само 6,5% у истраживању старијих користи интернет, а ниједан испитаник из ове образовне групе није навео да за приступ интернету користи рачунар, лаптоп, таблет или паметни телевизор. Ова група се највише ослања на традиционалне медије и личне контакте, што смањује разноврсност извора и могућност провере (Матовић и др., 2023).

Додатни проблем је ниска мотивација за формално унапређење вештина. У целокупној популацији 65+ тек 5,7% изражава жељу да унапреди медијску писменост, а 7,5% дигиталне вештине. Аутори студије описују став дела испитаника да су „стари за то”, што показује да је дигитални јаз истовремено инфраструктурни, образовни и мотивациони (Матовић и др., 2023). Због тога су за ову групу најпогоднији практични, локални и непосредни облици подршке, уз јасан доказ корисности за свакодневни живот.

Табела 5. Аналитичка типологија ризика по генерацији и образовању

Група	Предност	Главни ризик	Приоритет образовања
Млађи, више образовање	висока дигитална спретност, више извора	профилисање, алгоритми, ВИ, преоптерећење	напредна критичка и приватносна писменост
Млађи, ниже образовање	интензивна употреба платформи	изједначавање техничке спретности и критичности	провера извора, инфлуенсери, приватност на мрежама
Средње генерације, више образовање	комбиновање традиционалних и дигиталних извора	информационо преоптерећење, финансијске преваре	провера чињеница, сајбер-безбедност, подаци у услугама
Старији, више образовање	висока укљученост унутар своје генерације	нови облици преваре и ВИ садржај	циљана напредна дигитална подршка
Старији, ниже образовање	ослонац на познате медије и локалне мреже	дигитална искљученост, уски извори, ниска мотивација	непосредна практична обука и локална подршка

Извор: аутор, 2026.

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА КАО НОВИ ТЕСТ МЕДИЈСКЕ И ПРИВАТНОСНЕ ПИСМЕНОСТИ

Убрзано ширење генеративне вештачке интелигенције додатно повезује медијску писменост и приватност. Корисник више не процењује само садржај који је направио новинар, институција или други корисник, већ и текст, слику, аудио или видео који може бити синтетички генерисан. Истовремено, коришћење ВИ система подразумева уношење упита, докумената, фотографија и других података, што отвара нова питања приватности и свести о томе шта се сме делити са системом.

Истраживање из 2025. показује да платформе ВИ користи сваки четврти испитаник, али 71,9% свих испитаника наводи да никада не препознаје садржај направљен уз помоћ ВИ. Међу корисницима ВИ, 30% никада не проверава садржај пре прослеђивања, а исти проценат га не прилагођава пре прослеђивања (Матовић и др., 2025a). Пилот индекс је због тога димензију припремљености за ВИ оценио са само 23,42/100, најниже од свих шест димензија (Матовић и др., 2025b). Генерацијски јаз у ВИ може да понови стари дигитални јаз, али у новом облику. Млађи и образованији корисници вероватније ће раније усвојити ВИ алате и добити предност у раду и образовању, док старији и ниже образовани могу остати ван тог процеса. Међутим, рано усвајање носи и нове ризике: некритичко ослањање на генерисане одговоре, уношење осетљивих података и прецењивање тачности система. Зато се припремљеност за ВИ мора истовремено мерити кроз употребу, критичку процену и приватносну самозаштиту.

ДИСКУСИЈА

Синтеза доступних података показује да у Србији постоји сложена, а не линеарна веза између старости, образовања, медијске писмености и свести о приватности. Најједноставнији стереотип – да су млади медијски писмени јер користе интернет, а старији неписмени јер више гледају телевизију, није потврђен. Млади јесу технички спретнији и користе више дигиталних платформи, али најмлађа група показује слабију навику провере извора од млађих одраслих. Са друге стране, више и високо образовани старији грађани у великој мери користе интернет и имају медијски профил који се битно разликује од профила вршњака са нижим образовањем.

То указује на два различита дигитална јаз. Први је јаз приступа: да ли појединац уопште користи интернет, уређаје и дигиталне услуге. Он је и даље снажно присутан код дела старије и ниже образоване популације. Други је јаз квалитет употребе: да ли корисник уме да провери извор, препозна манипулацију, разуме алгоритамску логику, управља приватношћу и користи дигиталне могућности за активну партиципацију. Овај други јаз присутан је и међу онима који су свакодневно на интернету. Управо зато је ниво образовања кључни посредујући фактор. Образовање није само формални степен школовања, већ показатељ приступа ресурсима, когнитивних навика и друштвених могућности. Податак да међу старијима интернет користи 6,5% најниже образованих, а 85,9% више и високо образованих, вероватно је најјаснији доказ да генерацијски ефекат треба тумачити унутар социјалне структуре, а не изоловано.

Слична логика важи и за приватност. Старији, ниже образовани и рурални грађани у истраживању из 2023. идентификовани су као осетљивије групе. Њихова рањивост, међутим, не произлази само из мањег познавања подешавања приватности, већ и из мање изложености информацијама о правима, ужег избора извора и ниже мотивације за додатно учење. Насупрот томе, млађи и образованији имају више знања о техничким мерама, али су због већег обима дигиталних активности изложени већем броју ситуација у којима подаци могу бити прикупљени или злоупотребљени.

Зато медијску писменост и свест о приватности треба посматрати као динамичке компетенције. Нема групе која је једном заувек „писмена”. Промене платформи, појава ВИ, нови облици преваре и промене медијског тржишта могу брзо да учине постојеће знање недовољним. То је један од разлога што пилот индекс предлаже редовно национално мерење медијске писмености и системске програме који ће бити прилагођени конкретним дефицитима, а не универзалним претпоставкама о корисницима (Матовић и др., 2025b).

ПРЕПОРУКЕ

На основу анализираних налаза може се формулисати неколико праваца деловања. Први је увођење континуиране медијске и информационе писмености кроз образовни систем. Акценат не би требало да буде само на техничком коришћењу дигиталних алата, већ на провери извора, разумевању јавног интереса, препознавању оглашавања и манипулације, заштити података, ауторским правима и одговорном објављивању туђих садржаја.

Други правац је диференцирање програма према старосним и образовним групама. За адолесценте су приоритет алгоритми, инфлуенсери, визуелна манипулација, дељење фотографија и дигитални траг. За млађе одрасле потребни су напреднији садржаји о профилисању, ВИ и економији података. За средње генерације посебно су важни онлајн преваре, електронске услуге и провера садржаја у условима информационог преоптерећења. За старије је потребан двоструки приступ: напредни садржаји за образоване и већ дигитално активне и непосредна практична подршка за ниже образоване и дигитално искључене.

Трећи правац односи се на локалну доступност програма. Подаци показују да су рурална средина и ниже образовање често повезани са дигиталним искључивањем. Због тога библиотеке, домови културе, удружења пензионера, школе и локалне самоуправе могу бити важни носиоци обука које су бесплатне, практичне и прилагођене корисницима. Посебно је користан међугенерациски модел у коме млађи помажу у техничким питањима, а старији учествују као активни партнери, а не пасивни примаоци знања.

Четврти правац је јачање јавне комуникације о правима на приватност. Истраживање из 2023. показује велику потребу за конкретним информацијама: ко сме да тражи податке, коме се пријављује злоупотреба и која права грађанин има. Кампање треба да користе јасан језик, конкретне животне ситуације и медијске канале прилагођене циљним групама. За старије и ниже образоване није довољно поставити информацију на веб-сајт; потребни су телевизија, локални медији и непосредна подршка. Пети правац је повезивање медијске писмености са медијском одговорношћу. Од грађана се не може очекивати да индивидуалним вештинама компензују системско непоштовање професионалних стандарда. Зато су развој медијске писмености, квалитетно новинарство, ефикасна саморегулација, заштита података и медијски плурализам међусобно зависни. Грађанин који зна своја права има већу способност да препозна повреду приватности, али је неопходно да постоје институције и процедуре које ће то право стварно заштитити.

ЗАКЉУЧАК

Медијска писменост и свест грађана о заштити приватности у Србији показују исту основну структурну особину: постоји значајна разлика између приступа технологији и квалитета њене употребе. Већина грађана је укључена у медијско окружење и у великој мери препознаје да су дезинформације, злоупотреба података и нарушавање приватности реални ризици. Ипак, практичне навике провере и систематске мере самозаштите нису развијене у истој мери. Генерацијска припадност је важна јер усмерава медијске навике. Млади чешће живе у окружењу друштвених мрежа, видео-платформи и инфлуенсера, док старији више зависе од

телевизије и традиционалних извора. Али генерацијска припадност не одређује аутоматски ниво медијске писмености. Најмлађи корисници могу бити технички веома спретни, а ипак ретко проверавати извор. Са друге стране, високообразовани старији грађани могу бити веома активни корисници интернета и различитих дигиталних услуга. Ниво образовања се зато показује као један од најважнијих фактора. Он је повезан са ширином медијског репертоара, критичким читањем, дигиталним компетенцијама и активнијим стратегијама заштите приватности. Најизразитији пример је популација старија од 65 година, у којој интернет користи 6,5% испитаника са основним и нижим образовањем, а 85,9% више и високо образованих. Овај јаз показује да старост и образовање морају бити анализирани заједно. Основни закључак рада може се формулисати на следећи начин: генерација у великој мери одређује где грађанин долази до информација, док образовање значајно утиче на то шта ће са тим информацијама урадити. Развој медијске писмености и свести о приватности зато захтева доживотно учење, прилагођено различитим генерацијама и образовним нивоима. Уместо универзалних програма, потребне су циљане интервенције које повезују критичко мишљење, дигиталну безбедност, право на приватност и разумевање савременог медијског система.

РЕФЕРЕНЦЕ

Закон о заштити података о личности. (2018). Службени гласник Републике Србије, 87/2018. Доступно на: https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html (Приступљено: 31. августа 2026.)

Kantar Serbia I TMG Insights. (2023). Перцепција грађана о заштити података о личности: Други талас истраживања. Мисија ОЕБС-а у Србији. Доступно на: <https://serbia.osce.org/sites/default/files/f/documents/a/0/548512.pdf> (Приступљено: 18. августа 2026.)

Коматина, С., Раковић, Б., Јеремић, Ј. (2022). Грађани и медији: IV циклус. Нова писменост / CeSID. Доступно на: <https://novapismenost.propulsion.one/wp-content/uploads/2022/11/GRAD-JANI-I-MEDIJI-2022.pdf> (Приступљено: 12. августа 2026.)

Матовић, М., Милин Перковић, С., Јосифовић, С. (2023). Медијски корисници старији од 65 година у Србији. Друштво за креативне иницијативе RE.kreAKTa / Мисија ОЕБС-а у Србији. Доступно на: <https://www.osce.org/files/f/documents/3/2/541704.pdf> (Приступљено: 1. септембра 2026.)

Матовић, М., Милојевић, А., Милин Перковић, С., Томашевић, А., Јосифовић, С., & Јовић, М. (2025а). Медијска писменост грађана Србије: Извештај анкетног истраживања. Мисија ОЕБС-а у Србији. Доступно на: https://serbia.osce.org/sites/default/files/documents/official_documents/2026/01/2025%20Medijska%20pismenost%20gra%C4%91ana%20Srbije%2C%20Izve%C5%A1taj%20anketnog%20istra%C5%BEivanja_0.pdf (Приступљено: 4. септембра 2026.)

Матовић, М., Милојевић, А., Милин Перковић, С., Томашевић, А. (2025б). Индекс медијске писмености у Србији 2025 – пилот верзија. Мисија ОЕБС-а у Србији. Доступно на: https://serbia.osce.org/sites/default/files/documents/official_documents/2026/02/Izve%C5%A1taj%20Indeks%20medijske%20pismenosti%20u%20Srbiji%202025_FINAL.pdf (Приступљено: 5. септембра 2026.)

Савет за штампу. (2025). Кодекс новинара и новинарки Србије. Доступно на: <https://savetzastampu.rs/wp-content/uploads/2024/12/KODEKS-novinara-i-novinarki-2025-korekcija.pdf> (Приступљено: 25. августа 2026.)

Савет за штампу. (2026). Резултати рада Комисије за жалбе и мониторинга поштовања Кодекса новинара и новинарки Србије у дневним новинама од 1. јула до 31. децембра 2025. године. Доступно на: <https://savetzastampu.rs/lat/izvestaji/rezultati-rada-komisije-za-zalbe-i-monitoringa-postovanja-kodeksa-novinar-a-i-novinarki-srbije-u-dnevnim-novinama-od-1-jula-do-31-decembra-2025-godine-2/> (Приступљено: 19. августа 2026.)

UNESCO. (2025). Media and information literacy. UNESCO. Доступно на: <https://unesdoc.unesco.org/> (Приступљено: 11. маја 2026.)

European Commission. (n.d.). Media literacy. European Commission. Доступно на: https://ec.europa.eu/information_society/doc/factsheets/073-media-literacy.pdf (Приступљено: 13. јула 2026.)

САЈБЕР БЕЗБЕДНОСТ КАО ИЗАЗОВ САВРЕМЕНОГ МЕНАЏМЕНТА У УСЛОВИМА ДИГИТАЛНЕ ТРАНСФОРМАЦИЈЕ

Немања Деретић¹

Сажетак

Дигитална трансформација значајно мења начин функционисања савремених организација, утичући на пословне процесе, доношење одлука, управљање ресурсима, организациону структуру и односе са заинтересованим странама. Истовремено, интензивнија примена дигиталних технологија повећава изложеност организација различитим облицима сајбер претњи и ризика, због чега сајбер безбедност постаје једно од кључних питања савременог менаџмента. Циљ овог рада је да се анализира значај сајбер безбедности у условима дигиталне трансформације, са посебним освртом на управљање сајбер ризицима, улогу менаџмента, менаџерске компетенције и организациону културу. У раду се разматрају основни облици сајбер ризика у дигиталном пословном окружењу, укључујући неовлашћени приступ подацима, фишинг, уцењивачки софтвер, ризике повезане са новим технологијама, пословним континуитетом и људским фактором. Посебна пажња посвећена је потреби интегрисања сајбер безбедности у стратешко и оперативно управљање организацијом, као и усклађивању безбедносних активности са пословним циљевима, управљањем ризицима и расподелом ресурса. Анализа указује да ефикасно управљање сајбер ризицима захтева активно учешће највишег менаџмента, бољу сарадњу техничких и пословних функција и развој компетенција за разумевање пословних, финансијских и организационих последица сајбер претњи. Посебан значај има организациона култура сајбер безбедности, која кроз подршку руководства, јасне политике, обуке и развој свести запослених доприноси безбеднијем понашању. Закључује се да успешна дигитална трансформација захтева интегрисан развој технолошких, управљачких, организационих и безбедносних капацитета.

Кључне речи: сајбер безбедност, дигитална трансформација, менаџмент, сајбер ризици, менаџерске компетенције, организациона култура.

¹ Београдска академија пословних и уметничких струковних студија, Београд, Србија
e-mail: nemanja.deretic@bpa.edu.rs

УВОД

Дигитална трансформација постала је једно од кључних обележја савременог пословног окружења. Њена примена подразумева све шире укључивање дигиталних технологија у пословне процесе, комуникацију, доношење одлука, управљање ресурсима и односе са корисницима. Савремене технологије, као што су вештачка интелигенција, велики подаци и аналитика, блокчејн (енгл. *blockchain*), рачунарство у облаку (енгл. *cloud computing*), Интернет ствари (енгл. *Internet of Things* – IoT) и индустријски Интернет ствари (енгл. *Industrial Internet of Things* – IIoT), представљају важне покретаче дигиталне трансформације и омогућавају организацијама да повећају ефикасност, продуктивност и флексибилност пословања. Истовремено, интензивнија употреба информационих технологија (ИТ) повећава изложеност организација сајбер претњама, нападима и повредама безбедности података (Saeed et al., 2023).

Дигитална трансформација зато не може бити посматрана само као процес технолошког унапређења. Она утиче на све кључне функције менаџмента, укључујући предвиђање, планирање, организовање, вођење и контролу. Banciu et al. (2023) указују да дигиталне технологије омогућавају ефикасније прикупљање и анализу података, аутоматизацију процеса, унапређење сарадње и комуникације, као и праћење организационих перформанси у реалном времену. Међутим, аутори истичу да дигитална трансформација мора имати стратешки приступ који истовремено узима у обзир управљање ризицима, безбедност и адекватно управљање пројектима дигитализације (Banciu et al., 2023).

Са растућом зависношћу организација од информационих система, података и међусобно повезаних дигиталних инфраструктура, сајбер безбедност постаје важан предуслов пословног континуитета и успешне дигиталне трансформације. Saeed et al. (2023) наглашавају да дигитална трансформација, иако доприноси расту ефикасности и продуктивности, истовремено ствара нове ризике, укључујући повреде података и различите облике сајбер напада. Због тога организације морају да развијају одговарајући ниво сајбер спремности и да безбедносне мере укључе у сам процес дигиталне трансформације, а не да их посматрају као накнадну техничку активност (Saeed et al., 2023).

Савремена истраживања све више показују да ефикасна сајбер безбедност не зависи искључиво од техничких решења. Jonathan et al. (2024) указују да успешност управљања информационом безбедношћу зависи од више међусобно повезаних фактора, међу којима су лидерске вештине и ставови, организациона култура, организациона структура, управљање информационим технологијама (енгл. *IT governance*), усклађеност ИТ-а са пословним циљевима и праксе управљања људским ресурсима. Њихови налази такође показују да ефикасно управљање информационом безбедношћу има значајну улогу у остваривању успешне дигиталне трансформације (Jonathan et al., 2024). У том контексту, сајбер безбедност све више постаје питање стратешког и оперативног менаџмента. Magnusson et al. (2025) истичу да управљање информационом безбедношћу обухвата управљање ризицима, одговорност, усклађивање са стратегијом организације, контролу и заштиту критичних информационих ресурса. Стратешко усмеравање сајбер безбедности стога представља одговорност највишег менаџмента, који мора да обезбеди да ризици буду правилно идентификовани и контролисани, а ресурси одговорно коришћени.

Посебан изазов представља управљање сајбер ризицима, који се разликују од многих традиционалних пословних ризика по својој динамичности, сложености и потенцијалу да изазову значајне финансијске, оперативне и репутационе последице. Slapničar et al. (2025) сајбер

ризик сврставају међу значајне пословне ризике дигитализоване економије и наглашавају да његово стратешко управљање захтева учешће и разумевање највишег руководства. Истовремено, Shaikh и Siponen (2022) показују да пажња највишег менаџмента према сајбер безбедности има важну улогу у одлучивању о процени информационо-безбедносних ризика након безбедносних инцидената, јер је управо највиши менаџмент у позицији да распоређује ресурсе, сагледава пословне последице и координира активности на нивоу целе организације.

Поред структура управљања и процене ризика, све већи значај има и људски фактор. Сајбер безбедност није само технички проблем већ и питање организационе културе и понашања запослених. Sutton и Tompson (2025) наглашавају да развој снажне културе сајбер безбедности захтева укљученост највишег менаџмента, моделовање пожељног понашања и подршку целе организације. Слично томе, Grill et al. (2025) показују да обуке које укључују и менаџерско понашање могу позитивно утицати на информационо-безбедносно лидерство и организациону безбедносну културу.

Полазећи од наведеног, предмет овог рада је сајбер безбедност као изазов савременог менаџмента у условима дигиталне трансформације. Циљ рада је да се анализирају промене које дигитална трансформација доноси савременим организацијама, идентификују главни сајбер ризици и укаже на улогу менаџмента у њиховом препознавању, процени и контроли. Посебна пажња посвећена је менаџерским компетенцијама, организационој култури, управљању сајбер ризицима и значају укључивања руководства и запослених у развој одрживе сајбер безбедности.

Рад се састоји од шест делова. Након уводних разматрања, у другом делу анализира се дигитална трансформација као оквир савременог пословања. Трећи део посвећен је сајбер безбедности и ризицима у дигиталном пословном окружењу. У четвртном делу разматра се менаџмент сајбер безбедности у савременим организацијама, док је пети део посвећен менаџерским компетенцијама, организационој култури и управљању сајбер ризицима. У шестом делу изложена су закључна разматрања.

ДИГИТАЛНА ТРАНСФОРМАЦИЈА КАО ОКВИР САВРЕМЕНОГ ПОСЛОВАЊА

Дигитална трансформација представља један од најзначајнијих процеса који обликују савремено пословно окружење. Она не подразумева само увођење нових дигиталних технологија, већ ширу промену начина на који организације креирају вредност, организују пословне процесе, комуницирају са корисницима и доносе одлуке. Савремене организације све више користе вештачку интелигенцију, велике податке и аналитику, рачунарство у облаку, Интернет ствари и друге дигиталне технологије како би повећале ефикасност, флексибилност и способност прилагођавања променама на тржишту. Истовремено, дигитална трансформација омогућава развој нових облика сарадње и повезивања организација са купцима, добављачима, партнерима и другим заинтересованим странама, чиме се стварају услови за иновације и унапређење организационих перформанси (Jonathan et al., 2024; Saeed et al., 2023).

Суштина дигиталне трансформације огледа се у томе што технологија постаје интегрални део пословног модела, а не само средство за подршку појединачним активностима. Chotia et al. (2025) указују да дигитална трансформација мења начин на који организације обављају пословање коришћењем великих података и пословне аналитике, мобилних технологија, рачунарства у облаку, друштвених платформи и Интернета ствари. Такве промене утичу не

само на оперативне активности већ и на начин стварања и испоруке вредности, због чега организације морају да развијају нове динамичке способности, укључујући способност анализе података, интеграцију тимова и прилагођавање пословних процеса. Дигитална трансформација се, према томе, може посматрати као стратешки процес усмерен ка дугорочном унапређењу конкурентности, а не као једнократна технолошка модернизација (Chotia et al., 2025).

Посебан значај дигиталне трансформације огледа се у њеном утицају на класичне функције менаџмента. Banciu et al. (2023) истичу да дигиталне технологије мењају предвиђање, планирање, организовање, вођење и контролу. Коришћење података у реалном времену и напредних аналитичких алата омогућава менаџерима да квалитетније предвиђају тржишне промене и потенцијалне ризике, док дигитални алати за сарадњу олакшавају координацију запослених и организационих јединица. У области контроле, дигитални системи омогућавају континуирано праћење кључних показатеља перформанси и брже реаговање на одступања. Због тога дигитална трансформација утиче на све нивое менаџмента и захтева да руководиоци развијају нове приступе управљању и вођењу организација (Banciu et al., 2023).

Дигитална трансформација истовремено ствара нове могућности и нове изворе ризика. Повећана употреба рачунарства у облаку, Интернета ствари, мобилних система и других међусобно повезаних технологија доводи до веће зависности организација од података и информационих система. Са повећањем броја дигиталних компоненти и веза између њих расте и површина потенцијалног напада, па сајбер безбедност постаје један од основних предуслова успешне дигиталне трансформације. Saeed et al. (2023) наглашавају да дигитална трансформација може да повећа продуктивност и ефикасност организација, али истовремено отвара простор за повреде података, сајбер нападе и друге облике угрожавања пословног континуитета. Због тога се сајбер безбедност мора развијати паралелно са дигиталном трансформацијом, а не тек након увођења нових технологија (Saeed et al., 2023).

Међутим, успешност дигиталне трансформације не зависи искључиво од технолошке инфраструктуре. Значајну улогу имају организациони и менаџерски фактори, као што су лидерске способности, организациона култура, организациона структура, управљање информационим технологијама (енгл. *IT governance*), усклађивање информационих технологија са пословним циљевима и праксе управљања људским ресурсима. Jonathan et al. (2024) показују да ови фактори значајно утичу на ефикасност управљања информационом безбедношћу, али и на успешност саме дигиталне трансформације. Посебно се издвајају организациона култура, усклађеност ИТ-а са пословном стратегијом, лидерске способности и став руководства према информационој безбедности. То указује да организације не могу остварити пуне користи дигиталне трансформације уколико технолошке промене нису праћене одговарајућим организационим и управљачким прилагођавањем (Jonathan et al., 2024).

Поред технолошких и управљачких промена, успешна дигитална трансформација захтева и развој организационе способности за благовремено прилагођавање новим безбедносним захтевима. Jonathan et al. (2024) указују да ефикасно управљање информационом безбедношћу током дигиталне трансформације зависи од више институционалних и менаџерских фактора, као што су организациона агилност, дигитална стратегија, политика информационе безбедности, расположиви ресурси, интерна стручност, стил лидерства, управљање знањем и укљученост највишег менаџмента. Посебно је значајно усклађивање информационих технологија са пословном стратегијом, јер боља координација између ИТ функције и других организационих јединица доприноси ефикаснијој комуникацији, већој свести о безбедности и успешнијем остваривању користи од дигиталних инвестиција (Jonathan et al., 2024).

Развој дигиталних капацитета мора бити праћен и развојем организационе спремности за реаговање на променљиве сајбер претње. Safaeipour et al. (2026) истичу да сајбер спремност

не зависи само од појединачних обука или техничких мера, већ од координисаног деловања на нивоу запослених, тимова и целе организације. Обуке и активности усмерене на сајбер безбедност треба да буду повезане са реалним радним улогама, пословним процесима и свакодневним одлучивањем, како би се знање претворило у практично и доследно безбедносно понашање. На тај начин, сајбер безбедност постаје део стратешке и оперативне структуре организације, што доприноси већој отпорности и способности да се дигитална трансформација спроводи без нарушавања континуитета пословања (Safaeipour et al., 2026).

Са становишта савременог менаџмента, дигитална трансформација стога захтева интегрисан и стратешки приступ (табела 1). Није довољно само улагати у технологију, већ је неопходно истовремено управљати организационим променама, људским ресурсима, ризицима, информационом безбедношћу и пословном стратегијом. Banciu et al. (2023) наглашавају да успешна дигитална трансформација зависи од менаџерског разумевања процеса, начина управљања подацима и интеграције сајбер безбедности у управљачке функције. Слично томе, Jonathan et al. (2024) показују да су управљачки и организациони фактори тесно повезани са успешним управљањем информационом безбедношћу и остваривањем користи од дигиталне трансформације. Зато се дигитална трансформација може посматрати као свеобухватан организациони процес у којем су технологија, стратегија, људи, организациона култура и безбедност међусобно повезани елементи савременог пословања.

Табела 1. Кључне димензије дигиталне трансформације у савременом пословању

Димензија дигиталне трансформације	Основни садржај	Значај за савремено пословање	Извор
Примена савремених дигиталних технологија	Вештачка интелигенција, велики подаци и аналитика, рачунарство у облаку, Интернет ствари и друге дигиталне технологије	Унапређује ефикасност, продуктивност, флексибилност и могућности развоја нових услуга и пословних модела	Saeed et al. (2023); Chotia et al. (2025)
Трансформација пословних процеса	Аутоматизација, дигитализација активности, повезивање организационих функција и коришћење података у реалном времену	Омогућава брже извршавање процеса, бољу координацију и ефикасније доношење одлука	Banciu et al. (2023)
Трансформација функција менаџмента	Промене у предвиђању, планирању, организовању, вођењу и контроли	Омогућава менаџерима да брже реагују на промене и управљају организацијом на основу актуелних података	Banciu et al. (2023)
Стратешка и организациона трансформација	Повезивање технологије са пословном стратегијом, организационом структуром и културом	Обезбеђује да технолошке инвестиције буду усклађене са организационим циљевима и дугорочним развојем	Jonathan et al. (2024)
Развој нових организационих способности	Аналитичке способности, интегрисани тимови, нови облици сарадње и прилагођавања тржишним променама	Подржава иновације, конкурентност и способност организације да реагује на динамичне услове пословања	Chotia et al. (2025)

Информациона и сајбер безбедност	Заштита података, система, мрежа и дигиталних ресурса од унутрашњих и спољашњих претњи	Представља предуслов пословног континуитета и сигурног остваривања користи од дигиталне трансформације	Saeed et al. (2023); Jonathan et al. (2024)
Улога менаџмента	Стратешко усмеравање, расподела ресурса, управљање променама, ризицима и безбедношћу	Повезује технолошке, организационе и безбедносне аспекте дигиталне трансформације	Banciu et al. (2023); Jonathan et al. (2024)

Извор: Систематизација аутора на основу Banciu et al. (2023); Saeed et al. (2023); Jonathan et al. (2024); Chotia et al. (2025)

Из табеле 1 може се уочити да дигитална трансформација обухвата више међусобно повезаних димензија и да се њен утицај не своди само на примену савремених технологија. Поред увођења вештачке интелигенције, великих података, рачунарства у облаку и Интернета ствари, дигитална трансформација подразумева и промене у пословним процесима, функцијама менаџмента, организационој структури и начину доношења одлука. Посебно је значајно што дигиталне технологије омогућавају брже извршавање активности, бољу координацију, употребу података у реалном времену и развој нових организационих способности, чиме се стварају услови за већу ефикасност, иновације и конкурентност.

Истовремено, табела 1 показује да успешна дигитална трансформација зависи од усклађивања технолошких промена са пословном стратегијом, организационом културом, информационом безбедношћу и улогом менаџмента. Заштита података, система и дигиталних ресурса представља предуслов сигурног и континуираног пословања, док менаџмент има кључну улогу у стратешком усмеравању, расподели ресурса и управљању променама и ризицима. На основу тога може се закључити да дигитална трансформација представља свеобухватан организациони процес у којем су технологија, људи, стратегија, безбедност и менаџмент међусобно тесно повезани.

САЈБЕР БЕЗБЕДНОСТ И РИЗИЦИ У ДИГИТАЛНОМ ПОСЛОВНОМ ОКРУЖЕЊУ

Све већа зависност организација од дигиталних технологија, информационих система и података доводи до тога да сајбер безбедност постаје један од кључних предуслова стабилног и континуираног пословања. Сајбер напади могу бити усмерени на неовлашћен приступ, измену или уништавање осетљивих информација, прибављање финансијске користи или прекид редовних пословних процеса. Последице таквих инцидената не ограничавају се само на непосредну техничку штету, већ могу обухватити финансијске губитке, нарушавање репутације, повећање трошкова осигурања и негативне ефекте на пословне партнере и друге организације у оквиру ланца снабдевања. Због тога сајбер ризици представљају значајан део укупног пословног ризика савремених организација (Saeed et al., 2023).

Дигитална трансформација додатно повећава изложеност организација сајбер ризицима јер увођење нових технологија проширује број дигиталних ресурса, система и комуникационих

канала које је потребно заштитити. Посебне изазове стварају рачунарство у облаку, Интернет ствари, мобилне технологије, велики подаци и друге међусобно повезане технологије. Saeed et al. (2023) истичу да развој дигитализације може истовремено да повећа ефикасност пословања и број потенцијалних безбедносних слабости. Међу карактеристичним претњама издвајају се фишинг (енгл. *phishing*), уцењивачки софтвер (енгл. *ransomware*), неовлашћени приступ подацима и напади усмерени на приватност и поверљиве информације. Због тога се сајбер безбедност мора разматрати већ приликом планирања и увођења нових дигиталних решења, а не тек након настанка инцидента (Saeed et al., 2023).

Сложеност сајбер ризика произлази и из чињенице да се њихов ниво непрекидно мења у складу са развојем технологије, појавом нових претњи и променама у организационој инфраструктури. Islam et al. (2025) указују да управљање сајбер ризиком мора бити прилагођено специфичном контексту организације, укључујући њене пословне процесе, ресурсе, структуру, културу, токове података, спољне партнере, законске захтеве и ланац снабдевања. Процена ризика стога треба да обухвати не само техничке рањивости већ и питања приватности, пословног континуитета, организационе отпорности и способности организације да одржи функционисање својих критичних услуга у условима сајбер инцидента (Islam et al., 2025).

Сајбер ризик има и изразиту стратешку димензију. Slapničar et al. (2025) указују да процена сајбер ризика не би требало да буде ограничена само на техничку процену појединачних уређаја и система, већ је потребно сагледати могуће последице по критичне пословне процесе и организацију у целини. Недовољна сарадња између техничких стручњака и пословног менаџмента може довести до фрагментираног препознавања ризика и неадекватног одређивања приоритета. Због тога је неопходно повезати информације о претњама и рањивостима са проценом финансијских, оперативних и стратешких последица, како би менаџмент могао да доноси оправдане одлуке о прихватању, ублажавању или контроли појединих ризика (Slapničar et al., 2025).

Ради прегледнијег сагледавања најважнијих ризика који прате дигитално пословно окружење, у табели 2 систематизовани су основни облици сајбер ризика, њихови могући извори и најзначајније последице по организацију.

Табела 2. Основни сајбер ризици у дигиталном пословном окружењу

Врста сајбер ризика	Карактеристичан извор или облик претње	Могуће последице по организацију	Извор
Неовлашћени приступ и повреда података	Искористиве рањивости система, украдени приступни подаци, недовољна контрола приступа	Губитак поверљивости, измена или уништавање података, правне и репутационе последице	Saeed et al. (2023)
Фишинг и социјални инжењеринг	Обмањујуће поруке и поступци усмерени на кориснике и запослене	Крађа приступних података, неовлашћени приступ системима и нарушавање безбедности	Saeed et al. (2023)
Уцењивачки софтвер	Злонамерни софтвер којим се онемогућава приступ подацима или системима уз захтев за откуп	Прекид пословања, губитак приступа подацима, финансијски губици	Saeed et al. (2023)
Ризици нових и повезаних технологија	Рачунарство у облаку, Интернет ствари, 5G и друге нове технологије	Проширење површине напада, појава нових рањивости и сложеније управљање безбедношћу	Saeed et al. (2023)

Ризици пословног континуитета	Напад на критичне системе, сервисе или међусобно зависне дигиталне ресурсе	Прекид пословних процеса, немогућност пружања услуга и оперативни губици	Islam et al. (2025)
Финансијски и стратешки сајбер ризици	Значајни безбедносни инциденти и недовољно повезивање техничких и пословних процена	Финансијски губици, погрешна алокација ресурса и угрожавање стратешких циљева	Slapničar et al. (2025)
Ризици повезани са људским фактором	Недовољна свест, знање или небезбедно понашање запослених	Повећана вероватноћа успешног напада и неадекватног реаговања на инцидент	Saeed et al. (2023)

Извор: Систематизација аутора на основу Saeed et al. (2023); Islam et al. (2025); Slapničar et al. (2025)

Из приказа у табели 2 може се уочити да сајбер ризици имају техничку, људску, оперативну, финансијску и стратешку димензију. То показује да њихово управљање не може бити искључива надлежност ИТ стручњака, већ захтева координисан приступ различитих организационих функција и непосредно укључивање менаџмента. Овакво разумевање сајбер ризика представља основу за разматрање улоге менаџмента сајбер безбедности у наредном поглављу.

МЕНАЏМЕНТ САЈБЕР БЕЗБЕДНОСТИ У САВРЕМЕНИМ ОРГАНИЗАЦИЈАМА

Менаџмент сајбер безбедности у савременим организацијама подразумева систематско повезивање безбедносних активности са стратегијом, пословним циљевима, управљањем ризицима и механизмима одговорности. Информациона безбедност више се не посматра само као реактивна техничка функција, већ као део корпоративног управљања који захтева активно учешће највишег менаџмента. Magnusson et al. (2025) истичу да управљање информационом безбедношћу обухвата стратешко усмеравање, управљање ризицима, контролу и одговорност, као и усклађивање безбедносних политика са организационим циљевима. Посебан значај има јасно дефинисање одговорности, праћење и мерење резултата, спровођење процена ризика и усклађивање са релевантним стандардима и регулаторним захтевима. На тај начин, сајбер безбедност постаје интегрални део процеса управљања организацијом, а не изолована активност ИТ сектора (Magnusson et al., 2025).

Ефикасно управљање сајбер безбедношћу захтева и континуиран приступ током целог животног циклуса дигиталних система и пословних процеса. Al-Janabi et al. (2024) наглашавају значај приступа заснованог на ризику, у којем се претње и рањивости благовремено идентификују и приоритизују, а мере заштите усклађују са пословним циљевима организације. Поред тога, безбедносне активности треба интегрисати са постојећим управљачким процесима, стандардима и механизмима континуираног побољшања. То подразумева праћење нових претњи, ажурирање планова, анализу претходних инцидената и прилагођавање безбедносних мера променама у пословном и технолошком окружењу. Овакав приступ доприноси бољој алокацији ресурса, већој организационој отпорности и благовременијем реаговању на сајбер ризике (Al-Janabi et al., 2024).

Најважније активности менаџмента сајбер безбедности могу се систематизовати као што је приказано у табели 3.

Табела 3. Кључне активности менаџмента сајбер безбедности

Област управљања	Основна активност менаџмента	Значај за организацију	Извор
Стратешко управљање	Усклађивање сајбер безбедности са пословним циљевима и стратегијом	Обезбеђује да безбедносне мере подржавају остваривање организационих циљева	Magnusson et al. (2025); Al-Janabi et al. (2024)
Управљање ризицима	Идентификација, процена, приоритизација и третман сајбер ризика	Омогућава усмеравање ресурса на најзначајније претње и рањивости	Al-Janabi et al. (2024)
Одговорност и контрола	Дефинисање улога, одговорности, праћења и извештавања	Смањује нејасноће у поступању и јача управљачку одговорност	Magnusson et al. (2025)
Усклађеност са стандардима	Примена одговарајућих стандарда и регулаторних оквира	Доприноси уједначеном и систематском управљању безбедношћу	Magnusson et al. (2025); Al-Janabi et al. (2024)
Континуирано побољшање	Праћење претњи, анализа инцидената и ажурирање планова и контрола	Омогућава прилагођавање новим ризицима и технолошким променама	Al-Janabi et al. (2024)
Обука и развој спремности	Усклађивање обука са улогама, ризицима и свакодневним пословним процесима	Јача практичну спремност запослених и смањује ризике повезане са људским фактором	Safaeipour et al. (2026)

Извор: Систематизација аутора на основу Magnusson et al. (2025); Al-Janabi et al. (2024); Safaeipour et al. (2026)

Из табеле 3 може се видети да менаџмент сајбер безбедности обухвата много шири скуп активности од саме техничке заштите информационих система. Он повезује стратегију, управљање ризицима, одговорност, стандарде, континуирано побољшање и развој запослених, што потврђује да је сајбер безбедност у савременим организацијама пре свега организационо и менаџерско питање са снажном технолошком компонентом.

МЕНАЏЕРСКЕ КОМПЕТЕНЦИЈЕ, ОРГАНИЗАЦИОНА КУЛТУРА И УПРАВЉАЊЕ САЈБЕР РИЗИЦИМА

Управљање сајбер ризицима у савременим организацијама захтева да менаџери, поред класичних управљачких способности, поседују довољан ниво разумевања сајбер претњи, ризика и њихових пословних последица. Посебно су значајне способности тумачења информација о ризицима, повезивања техничких и пословних аспеката, одређивања приоритета, расподеле ресурса и координације активности различитих организационих функција. Shaikh и Sironen (2022) указују да највиши менаџмент има посебно важну улогу у процени информационо-безбедносних ризика, јер се налази у позицији да сагледа ризике у ширем пословном контексту, мобилише потребне ресурсе и координира активности на нивоу целе организације. Истовремено, Slapničar et al. (2025) показују да прекомерно ослањање на техничке стручњаке може довести до јаза између техничког разумевања претњи и стратешког разумевања њихових финансијских и пословних последица. На сличан проблем указују и Xin et al. (2026), који наглашавају постојање техничке и језичке баријере између тимова за сајбер безбедност и пословних тимова који доносе одлуке о инвестицијама и управљању ризицима. Њихов приступ настоји да сложене сајбер ризике изрази у финансијским категоријама и тако омогући јасније повезивање безбедносних приоритета са стратешким пословним циљевима организације.

Организациона култура представља други значајан елемент управљања сајбер ризицима, јер понашање запослених не зависи само од техничких мера и формалних правила, већ и од вредности, ставова, подршке руководства и начина на који се безбедност практично спроводи у организацији. Alshammari и Al-Mamary (2026) показују да организациона безбедносна култура значајно утиче на свест запослених о сајбер безбедности, док већа свест доприноси безбеднијем понашању. Посебно се издвајају посвећеност менаџмента, јасноћа политика и континуирано организационо подстицање безбедног понашања. Овакво становиште је у складу и са налазима Varghese и Bui (2026), који управљање информационо-безбедносним ризицима посматрају кроз три међусобно повезане перспективе: техничку, социо-бихејвиоралну и стратешко-управљачку. Такав приступ указује да ефикасно управљање сајбер ризицима захтева истовремено повезивање техничких контрола, понашања запослених и стратешког надзора менаџмента. Са тог становишта, менаџери имају двоструку улогу: да доносе одлуке о ризицима и ресурсима, али и да својим ставовима, комуникацијом и понашањем утичу на формирање културе у којој се сајбер безбедност прихвата као заједничка организациона одговорност (Alshammari & Al-Mamary, 2026; Varghese & Bui, 2026).

Sutton и Tompson (2025) додатно наглашавају да организациона култура сајбер безбедности не треба да се посматра само кроз постојање формалних политика, процедура и програма обуке, већ првенствено кроз њихов утицај на стварно понашање запослених. Аутори издвајају свест о претњама, мотивацију за безбедно поступање и способност запослених да адекватно реагују као важне елементе који повезују организациону културу и конкретно безбедносно понашање. Посебан значај имају посвећеност највишег менаџмента, праћење понашања, јасно дефинисана правила и подстицање запослених да активно учествују у заштити организације. То указује да развој културе сајбер безбедности захтева не само информисање запослених већ и стварање организационог окружења у којем се безбедно понашање систематски подржава и очекује (Sutton & Tompson, 2025).

Значај активне улоге менаџмента у развоју такве културе потврђују и Grill et al. (2025), који су испитивали ефекте програма обуке усмереног истовремено на запослене и руководиоце. Њихови

результати показују да обука која укључује и развој конкретних менаџерских образаца понашања може значајно да унапреди лидерство у области информационе безбедности и позитивно утиче на организациону безбедносну културу. Посебно се издваја значај практичног увежбавања пожељног понашања и повратних информација о учинку руководиоца, што указује да менаџери не утичу на сајбер безбедност само доношењем политика и одлука о ресурсима, већ и начином на који свакодневно усмеравају, подржавају и контролишу понашање запослених (Grill et al., 2025).

Ради прегледнијег приказа односа између менаџерских компетенција, организационе културе и управљања сајбер ризицима, у табели 4 издвојени су кључни елементи који доприносе ефикаснијој сајбер безбедности организације.

Табела 4. Кључне менаџерске компетенције и организациони фактори у управљању сајбер ризицима

Компетенција / организациони фактор	Основни садржај	Значај за управљање сајбер ризицима	Извор
Разумевање сајбер ризика	Разумевање претњи, рањивости и њихових пословних последица	Омогућава менаџменту да сајбер ризик посматра као пословни, а не само технички проблем	Slapničar et al. (2025)
Стратешко одлучивање	Одређивање приоритета, прихватљивог нивоа ризика и начина поступања	Омогућава усклађивање сајбер безбедности са пословним циљевима организације	Shaikh & Siponen (2022); Slapničar et al. (2025)
Расподела ресурса	Усмеравање финансијских, техничких и људских ресурса према приоритетним ризицима	Повећава ефикасност мера заштите и процена ризика	Shaikh & Siponen (2022)
Комуникација и координација	Повезивање техничких стручњака, руководства и других организационих функција	Смањује јаз између техничких информација и пословног одлучивања	Slapničar et al. (2025)
Посвећеност менаџмента	Видљива подршка политикама и активностима сајбер безбедности	Јача свест запослених и подстиче безбедно понашање	Alshammari & Al-Mamary (2026)
Организациона култура сајбер безбедности	Заједничке вредности, норме, правила и подршка безбедном понашању	Доприноси развоју свести и смањењу ризика повезаних са људским фактором	Alshammari & Al-Mamary (2026)
Свест и континуирано учење	Разумевање претњи и способност правилног реаговања	Претвара запослене из потенцијалне слабости у активни део организационе заштите	Alshammari & Al-Mamary (2026)

Извор: Систематизација аутора на основу Shaikh и Siponen (2022); Slapničar et al. (2025); Alshammari и Al-Mamary (2026)

Из табеле 4 може се закључити да ефикасно управљање сајбер ризицима зависи од комбинације менаџерских компетенција и организационих услова. Посебно су важни разумевање ризика, способност стратешког одлучивања, расподела ресурса и комуникација са техничким стручњацима, док организациона култура и подршка руководства утичу на то како ће се правила и мере сајбер безбедности заиста примењивати у свакодневном раду.

ЗАКЉУЧАК

Дигитална трансформација значајно мења начин функционисања савремених организација и све више повезује пословне процесе, информационе системе, податке и нове технологије. Иако такве промене доносе бројне користи у погледу ефикасности, флексибилности, бржег доношења одлука и развоја нових пословних модела, истовремено повећавају изложеност организација различитим облицима сајбер ризика. Због тога сајбер безбедност више не може бити посматрана као искључиво техничко питање, већ као важан део стратегије, управљања ризицима и обезбеђивања пословног континуитета. Ефикасно управљање сајбер безбедношћу захтева системски приступ који обухвата идентификацију и процену ризика, стратешко усмеравање, јасно дефинисане одговорности, примену релевантних стандарда, континуирано праћење претњи и унапређивање безбедносних мера. Посебно је значајно да највиши менаџмент буде активно укључен у процесе одлучивања, расподелу ресурса и повезивање техничких информација са пословним и финансијским последицама. Истовремено, организације треба да развијају културу у којој се сајбер безбедност прихвата као заједничка одговорност свих запослених, а не само ИТ стручњака. На основу разматраних истраживања може се закључити да су менаџерске компетенције, организациона култура и управљање сајбер ризицима међусобно тесно повезани. Савремени менаџери морају да разумеју природу сајбер претњи, њихове пословне последице и могућности управљања ризицима, али и да развијају комуникацију, координацију, свест и безбедносно одговорно понашање у организацији. Успешна дигитална трансформација стога зависи не само од квалитета технолошких решења већ и од способности организације да истовремено развија управљачке, организационе и безбедносне капацитете.

РЕФЕРЕНЦЕ

- Al-Janabi, S., Jabbar, H., & Syms, F. (2024). Cybersecurity transformation: cyber-resilient IT project management framework. *Digital*, 4(4), 866–897. <https://doi.org/10.3390/digital4040043>
- Alshammari, M. M., & Al-Mamary, Y. H. (2026). Cybersecurity Awareness as a Mediating Factor in the Human Firewall System. *Computers in Human Behavior Reports*, 101118. <https://doi.org/10.1016/j.chbr.2026.101118>
- Banciu, D., Vevera, A. V., & Popa, I. (2023). Digital transformation impact on organization management and several necessary protective actions. *Studies in Informatics and Control*, 32(1), 49–56. <https://doi.org/10.24846/v32i1y202305>
- Chotia, V., Khoualdi, K., Broccardo, L., & Yaqub, M. Z. (2025). The role of cyber security and digital transformation in gaining competitive advantage through Strategic Management Accounting. *Technology in Society*, 81, 102851. <https://doi.org/10.1016/j.techsoc.2025.102851>
- Grill, M., Sommestad, T., Karlzén, H., & Pousette, A. (2025). Training for improved information security culture: a longitudinal randomized controlled trial. *Information & Computer Security*, 33(5), 690–718. <https://doi.org/10.1108/ICS-08-2024-0189>
- Islam, S., Basheer, N., Papastergiou, S., Ciampi, M., & Silvestri, S. (2025). Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. *Journal of Reliable Intelligent Environments*, 11(3), 12. <https://doi.org/10.1007/s40860-025-00253-3>
- Jonathan, G. M., Perjons, E., & Rusu, L. (2024). Untangling the link between digital transformation and information security management. *Procedia Computer Science*, 239, 575–582. <https://doi.org/10.1016/j.procs.2024.06.209>
- Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. *International Journal of Information Security*, 24(4), 177. <https://doi.org/10.1007/s10207-025-01097-x>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 6666. <https://doi.org/10.3390/s23156666>
- Safaeipour, M., Abhari, K., Huynh, N., Wu, C., & Fathi, F. (2026). Cybersecurity training governance: The SEAL Framework for sustained readiness. *Business Horizons*. <https://doi.org/10.1016/j.bushor.2026.02.002>
- Shaikh, F. A., & Siponen, M. (2022). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974. <https://doi.org/10.1016/j.cose.2022.102974>
- Slapničar, S., Axelsen, M., & Eulerich, M. (2025). Cyber risk management: an illusion of a risk-based approach. *Journal of Management Control*, 1-36. <https://doi.org/10.1007/s00187-025-00401-z>
- Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*, 148, 104110. <https://doi.org/10.1016/j.cose.2024.104110>
- Varghese, B. B., & Bui, Q. (2026). An integrated framework for information security risk management: A mixed-methods systematic literature review. *Computers & Security*, 104957. <https://doi.org/10.1016/j.cose.2026.104957>
- Xin, T., He, Y., Zamani, E. D., Evans, M., & Luo, C. (2026). A cyber risk economics model for organization-wide risk management (CYREM-ORM). *Computers & Security*, 104873. <https://doi.org/10.1016/j.cose.2026.104873>

ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА, АЛГОРИТМИ И ПРИВАТНОСТ ГРАЂАНА

Данијела Војиновић¹

Сажетак

Развој и примена вештачке интелигенције и дигиталне технологије доводи до суштинских промена у начинима прикупљања и обраде података о грађанима. Широка примена ових технологија у медијима, друштвеним мрежама и образовању доноси бројне могућности за персонализацију садржаја, ефикасније доношење одлука и унапређење процеса учења, али истовремено отвара значајна питања у погледу заштите приватности и основних људских права. Посебан изазов представља алгоритамско профилисање, којим се на основу прикупљених података могу предвиђати интересовања, понашање и карактеристике појединаца. Циљ рада је да се анализирају кључни изазови које примена вештачке интелигенције и алгоритамске обраде података поставља пред заштиту приватности грађана, са посебним освртом на медије и образовање. У раду се примењују дескриптивни метод, анализа садржаја релевантне научне и стручне литературе и компаративна анализа регулаторних решења у области заштите података и вештачке интелигенције. Додатна пажња усмерена је на питања која тангирају транспарентност алгоритама, контролу личних података, аутоматизованог доношења одлука и заштите података деце и младих у образовном простору. У раду се указује на потребу успостављања равнотеже између технолошких иновација и очувања права на приватност, уз јачање правних, етичких и образовних механизма за одговорну примену вештачке интелигенције.

Кључне речи: вештачка интелигенција, алгоритамско профилисање, приватност, лични подаци, медији, образовање.

¹ Факултет за образовање учитеља и васпитача Универзитета у Београду
e-mail: danijelavojinovic14@gmail.com

УВОД

Дигитална трансформација друштва довела је до интензивне примене технологија заснованих на вештачкој интелигенцији у различитим областима свакодневног живота. Системи вештачке интелигенције данас се користе за анализу великих количина података, препознавање образаца, предвиђање понашања и аутоматизовање различитих процеса, чиме се отварају значајне могућности за унапређење друштвених, економских и образовних процеса. Истовремено, све већа зависност ових система од великих количина података доводи до нових изазова у погледу контроле над личним подацима и заштите права на приватност (Jobin et al., 2019; UNESCO, 2021). Посебно значајан аспект представља алгоритамско профилисање, односно аутоматизована обрада података чији је циљ процена или предвиђање одређених карактеристика, интересовања или понашања појединаца. Алгоритми који се користе у дигиталним платформама могу на основу активности корисника да креирају детаљне профиле и да их користе за персонализацију садржаја, оглашавање или доношење различитих одлука. Иако такви механизми могу допринети ефикаснијем пружању услуга и прилагођавању дигиталног садржаја потребама корисника, они истовремено повећавају ризик од нарушавања приватности, недостатка транспарентности и губитка контроле појединаца над сопственим подацима (Mittelstadt et al., 2016; Zuboff, 2019).

Проблем постаје нарочито изражен у медијском окружењу и на друштвеним мрежама, где алгоритми анализирају велики број података о понашању корисника како би одредили који ће им садржаји бити приказани. Алгоритамска персонализација може утицати не само на избор информација које појединац прима већ и на начин на који се формира његово информисање и учешће у дигиталном јавном простору.

Прикупљање података о корисницима ради циљаног оглашавања и персонализације садржаја отвара питања граница прихватљиве обраде личних података и транспарентности начина на који алгоритамски системи функционишу (Helberger et al., 2018; Napoli, 2019). Вештачка интелигенција све интензивније налази примену и у области образовања. Интелигентни образовни системи, платформе за персонализовано учење, аутоматизовано оцењивање и генеративни алати засновани на вештачкој интелигенцији могу допринети прилагођавању наставе индивидуалним потребама ученика и студената. Међутим, њихова примена подразумева прикупљање и анализу различитих података о корисницима, укључујући податке о постигнућима, активностима, понашању и начину учења. Посебан проблем представља чињеница да су корисници образовних система често деца и млади, што захтева посебно висок ниво заштите њихових личних података и права на приватност (UNESCO, 2021; European Commission, 2022). Питање приватности у контексту вештачке интелигенције зато превазилази технички аспект заштите података и постаје питање заштите основних људских права. Могућност аутоматизованог доношења одлука, профилисања и предвиђања понашања појединаца захтева успостављање механизма транспарентности, одговорности и људског надзора над алгоритамским системима. Европски регулаторни приступ последњих година све више настоји да успостави равнотежу између подстицања технолошких иновација и заштите основних права, што је посебно видљиво кроз развој регулаторног оквира за заштиту података и вештачку интелигенцију (European Parliament & Council of the European Union, 2016, 2024).

Предмет овог рада јесте анализа односа између вештачке интелигенције, алгоритамског профилисања и заштите приватности грађана у дигиталном окружењу, са посебним освртом на примену ових технологија у медијима и образовању.

Циљ рада је да се идентификују и анализирају најзначајнији ризици које алгоритамска обрада података и системи вештачке интелигенције представљају за приватност грађана, као и да се сагледају могућности за њихово ублажавање кроз одговарајуће правне, етичке, технолошке и образовне механизме.

У складу са постављеним предметом и циљем, рад настоји да одговори на следећа истраживачка питања:

- (1) на који начин примена вештачке интелигенције и алгоритамског профилисања утиче на приватност грађана;
- (2) који су најзначајнији ризици по приватност у медијском и образовном окружењу; и
- (3) који механизми могу допринети одговорној и безбедној примени вештачке интелигенције уз очување права на приватност.

ТЕОРИЈСКИ ДЕО

Вештачка интелигенција у савременом дигиталном окружењу

Вештачка интелигенција представља једну од најзначајнијих технологија савременог дигиталног друштва, чија се примена из традиционалних области аутоматизације и анализе података проширила на готово све сегменте друштвеног живота. Савремени системи вештачке интелигенције заснивају се на способности алгоритама да обрађују велике количине података, препознају сложене обрасце, генеришу предвиђања и производе резултате који могу подржати или делимично аутоматизовати људско доношење одлука.

Развој машинског учења и дубоког учења додатно је унапредио могућности ових система, нарочито у областима препознавања слика и говора, обраде природног језика и анализе понашања корисника (Jordan & Mitchell, 2015; UNESCO, 2021). Иако се концепт вештачке интелигенције развија деценијама, њена савремена експанзија у великој мери је условљена доступношћу великих количина података, развојем рачунарске инфраструктуре и напретком алгоритама машинског учења. Подаци представљају један од основних ресурса за функционисање савремених AI система, јер омогућавају њихово обучавање, прилагођавање и континуирано унапређивање. Управо због тога дигитално окружење у којем грађани свакодневно користе интернет, друштвене мреже, дигиталне платформе и различите онлајн услуге постаје значајан извор података за алгоритамску анализу (Kitchin, 2017).

Посебан значај има развој генеративне вештачке интелигенције, која омогућава креирање текста, слика, аудио и видео садржаја на основу претходно обрађених података. Њена масовна доступност довела је до брзог ширења примене AI алата у медијима, привреди, јавном сектору и образовању. У образовном контексту генеративна AI може пружити подршку наставницима и ученицима кроз креирање образовних материјала, персонализацију учења и пружање повратних информација, али истовремено отвара питања у вези са заштитом личних података, ауторством, поузданошћу информација и одговорним коришћењем технологије (UNESCO, 2023). Развој вештачке интелигенције, међутим, не може се посматрати искључиво кроз призму технолошког напретка. Начин на који се AI системи развијају и користе има непосредне

импликације на појединце и друштво. Алгоритамски системи могу доносити или подржавати одлуке које утичу на приступ информацијама, образовању, услугама и другим друштвеним ресурсима. При томе корисници често немају довољно информација о томе који се подаци прикупљају, на који начин се анализирају и како се добијени резултати користе. Овај проблем постаје посебно значајан када алгоритамска обрада укључује личне податке или омогућава извођење закључака о појединцу на основу његовог дигиталног понашања (Mittelstadt et al., 2016).

У том смислу, развој вештачке интелигенције ствара двоструки изазов. Са једне стране, АИ представља значајан потенцијал за унапређење ефикасности, доступности информација и квалитета услуга, укључујући медије и образовање. Са друге стране, њена све већа зависност од података повећава могућност масовног прикупљања, повезивања и анализе информација о појединцима. Због тога се питање заштите приватности мора посматрати као један од централних услова одговорног развоја и примене вештачке интелигенције (UNESCO, 2021).

Алгоритми, аутоматизована обрада података и алгоритамско профилисање

Алгоритми представљају скуп правила и поступака који одређују начин на који се улазни подаци обрађују ради добијања одређеног резултата. У контексту вештачке интелигенције алгоритми могу бити изузетно сложени и способни да на основу великих количина података идентификују обрасце који нису непосредно видљиви човеку. Њихова примена омогућава аутоматизацију процеса који су раније захтевали значајно људско ангажовање, али истовремено поставља питање начина на који се алгоритамски резултати формирају и контролишу (Kitchin, 2017). Алгоритамско профилисање представља један од најзначајнијих начина на који савремене дигиталне технологије могу утицати на приватност појединца. На основу података о активностима корисника, њиховим претрагама, интеракцијама, интересовањима, локацији или другим карактеристикама, алгоритми могу креирати профиле који се користе за предвиђање понашања или персонализацију садржаја и услуга. Такав процес може бити користан када омогућава прилагођавање услуга индивидуалним потребама, али може довести и до ситуације у којој појединац није у потпуности свестан обима и последица обраде сопствених података (Wachter & Mittelstadt, 2019).

Посебно питање представља аутоматизовано доношење одлука. Када алгоритамски системи учествују у процени или класификацији појединаца, резултат такве обраде може имати директне последице по њихова права и могућности. Ризик се додатно повећава када су критеријуми према којима систем функционише недовољно транспарентни или када корисник нема реалну могућност да разуме и оспори донету одлуку. Због тога транспарентност, објашњивост и могућност људске интервенције представљају важне принципе одговорне примене алгоритамских система (European Commission, 2019). У медијском окружењу алгоритамско профилисање има посебан значај јер платформе могу анализирати понашање корисника како би им приказале персонализоване вести, огласе и друге садржаје. На тај начин алгоритми посредују између корисника и информација које он добија, што отвара не само питање приватности већ и питања аутономије појединца, транспарентности и утицаја на информисање јавности (Helberger et al., 2018). Сличан принцип може се применити и у образовању. Образовне платформе могу прикупљати податке о резултатима ученика, времену

проведеном у учењу, начину решавања задатака и другим аспектима њихове активности. Анализа ових података може омогућити персонализацију наставе и рано препознавање образовних тешкоћа, али истовремено ствара детаљне дигиталне профиле ученика. Посебну пажњу захтевају ситуације у којима се обрађују подаци деце и малолетних лица, јер њихова способност разумевања дугорочних последица обраде личних података може бити ограничена (UNESCO, 2023).

Право на приватност и заштита личних података

Право на приватност представља једно од основних људских права, а дигитализација друштва проширила је његов значај на питања прикупљања, чувања, обраде и размене личних података. У савременом дигиталном окружењу приватност више није ограничена на заштиту од непосредног мешања у лични и породични живот, већ обухвата и могућност појединца да има одређени степен контроле над информацијама које се односе на њега. Посебно значајан корак у развоју европског система заштите података представља Општа уредба о заштити података – GDPR, која успоставља принципе законитости, правичности и транспарентности обраде података, ограничења сврхе, минимизације података, тачности, ограничења чувања, интегритета и поверљивости (European Parliament & Council of the European Union, 2016). Ови принципи имају посебан значај у контексту вештачке интелигенције, јер се AI системи често ослањају на велике количине података и могу омогућити извођење нових информација о појединцима.

Увођење ризично заснованог приступа вештачкој интелигенцији додатно је наглашено усвајањем Акта Европске уније о вештачкој интелигенцији (EU AI Act), којим се успостављају хармонизована правила за развој и употребу система вештачке интелигенције и различити нивои регулаторних захтева у зависности од степена ризика који одређена примена носи (European Parliament & Council of the European Union, 2024). На тај начин заштита приватности постаје део ширег система управљања ризицима повезаним са AI технологијама. Проблем приватности посебно је сложен када појединац није у могућности да у потпуности разуме начин на који алгоритам користи његове податке. Сложеност савремених система машинског учења може отежати објашњење процеса који доводи до одређеног резултата, што може створити такозвани проблем „црне кутије”. Недовољна транспарентност може умањити могућност појединца да контролише коришћење својих података и да реагује у случају неправилности или дискриминаторних исхода (Wachter et al., 2017). Због тога заштита приватности у ери вештачке интелигенције захтева не само техничке мере безбедности већ и правне и етичке механизме који обезбеђују транспарентност, одговорност и могућност људског надзора над алгоритамским процесима.

Вештачка интелигенција, медији и друштвене мреже

Медији и друштвене мреже представљају једно од најзначајнијих подручја примене алгоритамских система. Савремене дигиталне платформе користе алгоритме за селекцију, рангирање и препоручивање садржаја, при чему се избор често заснива на подацима о претходним активностима и интересовањима корисника. На тај начин алгоритми не делују само као технички механизми за управљање великим бројем информација, већ постају посредници у процесу информисања грађана (Napoli, 2019). Прикупљање података за потребе персонализације садржаја може допринети релевантнијем корисничком искуству, али истовремено омогућава израду детаљних профила корисника. Комбиновањем различитих извора података могуће је закључивати о интересовањима, навикама и потенцијалном понашању појединаца. Такав модел дигиталног пословања повезује економску вредност података са питањима приватности и контроле над личним информацијама (Zuboff, 2019). Поред тога, алгоритамска персонализација може утицати на информационо окружење у којем се грађани крећу. Корисник не добија нужно исти садржај као други корисници, већ му се информације селектују на основу алгоритамске процене његових интересовања и понашања. Због тога се питање алгоритама у медијима не односи само на заштиту личних података, већ и на шири проблем аутономије корисника и квалитета информисања у дигиталном јавном простору.

Примена вештачке интелигенције у образовању и ризици по приватност

Образовање представља област у којој примена вештачке интелигенције има значајан потенцијал за унапређење наставног процеса. AI системи могу омогућити персонализацију учења, анализу постигнућа ученика, аутоматизовано пружање повратних информација и подршку наставницима у припреми образовних материјала. Генеративна вештачка интелигенција додатно је проширила могућности примене ових технологија, омогућавајући ученицима и наставницима интерактивну комуникацију и генерисање различитих образовних садржаја (UNESCO, 2023). Међутим, персонализација образовања заснована на вештачкој интелигенцији подразумева прикупљање и анализу података о ученицима и студентима. Ти подаци могу обухватати оцене, резултате тестова, време проведено на платформи, начине решавања задатака, интересовања, интеракције са образовним садржајима и друге информације које омогућавају формирање индивидуалног профила. Иако таква анализа може помоћи наставнику да боље разуме потребе ученика, она истовремено ствара ризик од прекомерног прикупљања и дуготрајног чувања података. Посебно осетљив проблем представља алгоритамско предвиђање образовних исхода. Уколико се на основу претходних података предвиђа успех ученика, ризик од погрешне класификације или стварања трајних профила може утицати на очекивања наставника и институција према одређеном ученику. Због тога примена AI у образовању мора бити заснована на принципима пропорционалности, транспарентности, недискриминације и заштите најбољег интереса детета. Поред заштите личних података, образовни сектор се суочава и са потребом развоја компетенција за одговорно коришћење вештачке интелигенције. Ученици и студенти треба да буду оспособљени да разумеју не само могућности AI алата већ и ризике који произилазе из њиховог коришћења,

укључујући питања приватности, безбедности података, поузданости генерисаног садржаја и алгоритамске пристрасности. У том смислу, дигитална и AI писменост постају важан елемент заштите приватности, јер информисан корисник лакше препознаје ризике и доноси одговорније одлуке о дељењу својих података (UNESCO, 2021, 2023).

Етички и правни изазови примене вештачке интелигенције

Примена вештачке интелигенције поставља бројна етичка питања која превазилазе проблем саме техничке функционалности система. Међу најзначајнијим изазовима издвајају се транспарентност, одговорност, правичност, недискриминација, објашњивост и заштита приватности.

Посебан проблем представља утврђивање одговорности у ситуацијама када алгоритамски систем произведе штетан или неправичан резултат, нарочито када је процес доношења одлуке сложен и тешко разумљив крајњем кориснику (Jobin et al., 2019). Етички принципи су због тога постали важан део савремених приступа управљању вештачком интелигенцијом. Међународне организације и институције развијају смернице које наглашавају људски надзор, транспарентност, безбедност, приватност и недискриминацију као кључне услове одговорне примене AI. Ипак, етичке смернице саме по себи нису довољне уколико нису праћене јасним правним обавезама, институционалним механизмима контроле и одговорношћу актера који развијају и користе AI системе (UNESCO, 2021).

МЕТОДОЛОГИЈА

Предмет истраживања у овом раду јесте однос између примене вештачке интелигенције, алгоритамског профилисања и заштите приватности грађана у савременом дигиталном окружењу, са посебним освртом на медије, друштвене мреже и образовни систем. Истраживање је усмерено на сагледавање начина на који алгоритамска обрада података може утицати на приватност појединаца, као и на идентификовање правних, етичких и друштвених изазова који настају применом ових технологија.

Циљ истраживања је да се анализирају најзначајнији ризици по приватност грађана који произилазе из примене система вештачке интелигенције и алгоритамског профилисања, као и да се сагледају могућности за одговорну примену ових технологија у медијском и образовном окружењу. Посебна пажња усмерена је на питања прикупљања и обраде личних података, транспарентности алгоритамских система, аутоматизованог доношења одлука, заштите података деце и младих и развоја дигиталне и AI писмености.

У складу са дефинисаним предметом и циљем истраживања, постављена су следећа истраживачка питања:

ИП1: На који начин примена вештачке интелигенције и алгоритамског профилисања утиче на приватност грађана?

ИП2: Који су најзначајнији ризици по приватност грађана у примени алгоритамских система у медијском и образовном окружењу?

ИП3: Који правни, етички и организациони механизми могу допринети одговорној примени вештачке интелигенције уз очување права на приватност?

ИП4: На који начин образовање и развој дигиталне и AI писмености могу допринети бољој заштити приватности грађана у дигиталном окружењу?

У раду је примењен **дескриптивни метод**, којим су представљени основни појмови и карактеристике вештачке интелигенције, алгоритамског профилисања, обраде личних података и права на приватност. Овај метод омогућио је систематизацију кључних теоријских поставки и идентификовање основних ризика повезаних са применом AI система. Примењен је и **метод анализе садржаја**, који је коришћен за анализу научних и стручних публикација, релевантних извештаја међународних организација, као и правних и стратешких докумената који регулишу или разматрају примену вештачке интелигенције и заштиту личних података. Посебна пажња посвећена је изворима који се односе на примену AI у медијима и образовању.

Компаративни метод коришћен је за сагледавање различитих приступа регулисању вештачке интелигенције и заштите приватности, пре свега кроз анализу европског регулаторног оквира и релевантних принципа одговорне примене AI. У том контексту разматрани су Општа уредба о заштити података (GDPR) и Акт Европске уније о вештачкој интелигенцији (EU AI Act), као значајни инструменти савременог приступа управљању ризицима повезаним са обрадом личних података и употребом AI система. Истраживање је засновано на **секундарним изворима података**, пре свега научним и стручним радовима, монографијама, зборницима радова, извештајима међународних организација и релевантним правним документима. При избору научне литературе примењен је критеријум актуелности, при чему су као приоритет коришћени извори објављени у периоду од **2016. до 2026. године**, како би се обезбедила релевантност анализе у односу на брз развој технологија вештачке интелигенције. Методолошки приступ омогућава повезивање технолошког, правног, етичког и образовног аспекта проблема приватности. На тај начин вештачка интелигенција није посматрана искључиво као технолошка иновација, већ као феномен који утиче на остваривање основних права грађана и захтева истовремено деловање законодаваца, медијских организација, образовних институција, технолошког сектора и самих корисника дигиталних технологија.

ДИСКУСИЈА

Анализа представљена у претходним поглављима показује да развој вештачке интелигенције и све интензивнија примена алгоритамских система доносе значајне користи за савремено дигитално друштво, али истовремено стварају нове и сложене ризике за приватност грађана. Основни проблем не произилази само из чињенице да се лични подаци прикупљају и обрађују, већ и из могућности да се њиховим повезивањем и алгоритамском анализом изводе нови закључци о појединцима. На тај начин појединачни подаци који сами по себи можда не представљају значајан ризик могу, када се комбинују са другим изворима, довести до стварања веома детаљних профила корисника (Wachter & Mittelstadt, 2019).

Одговор на прво истраживачко питање указује да вештачка интелигенција утиче на приватност грађана пре свега кроз повећање обима, брзине и сложености обраде података. Савремени алгоритми могу обрађивати велике количине информација и идентификовати обрасце понашања који нису непосредно видљиви кориснику. Проблем се додатно усложњава када грађанин није у потпуности свестан који се подаци о њему прикупљају, у које сврхе се користе и колико дуго се чувају. Стога традиционално разумевање пристанка корисника постаје све сложеније у условима дигиталних платформи и аутоматизоване обраде података. Посебно значајан ризик представља алгоритамско профилисање. Иако оно може имати позитивну функцију, попут персонализације садржаја и услуга, профилисање истовремено може довести до категоризације појединаца на основу њиховог понашања и претпостављених карактеристика. Уколико се алгоритамски модели заснивају на непотпуним или пристрасним подацима, могу настати неправични или дискриминаторни резултати. Ово показује да заштита приватности није изоловано питање, већ је непосредно повезана са принципима једнакости, недискриминације и аутономије појединца (Mittelstadt et al., 2016; Jobin et al., 2019).

У односу на друго истраживачко питање, медији и друштвене мреже представљају посебно значајно окружење за анализу ових ризика. Алгоритми за препоручивање садржаја омогућавају корисницима да брже дођу до информација које су им релевантне, али истовремено посредују у избору садржаја који корисник види. На тај начин персонализација може имати двоструки ефекат: повећава корисност дигиталних услуга, али истовремено повећава зависност корисника од алгоритамских процена. Уколико се персонализација заснива на интензивном праћењу корисничког понашања, питање заштите приватности постаје неодојиво од питања транспарентности рада дигиталних платформи (Helberger et al., 2018; Napolì, 2019). У образовању се појављује слична, али специфична ситуација. Примена вештачке интелигенције може допринети персонализацији учења, раном идентификовању тешкоћа у савладавању градива и ефикаснијем праћењу образовног напретка. Међутим, да би се такве могућности реализовале, образовне платформе могу прикупљати велики број података о активностима ученика и студената. Подаци о резултатима, начину учења, времену проведену у раду и интеракцијама са дигиталним садржајима могу омогућити формирање веома детаљног профила ученика. Ово отвара питање границе између корисне персонализације наставе и прекомерног надзора над ученицима (UNESCO, 2023).

Посебно осетљиву категорију представљају деца и млади, јер последице обраде њихових података могу бити дугорочне. Ученици често немају довољно знања и искуства да у потпуности процене последице дељења личних података са дигиталним платформама. Због тога одговорност за заштиту приватности у образовању не може бити пребачена искључиво на појединца. Образовне институције, наставници и пружаоци дигиталних услуга морају успоставити јасна правила у погледу прикупљања, коришћења и чувања података ученика. У том смислу, четврто истраживачко питање, које се односи на улогу образовања у заштити приватности, има посебан значај. Дигитална и AI писменост не треба да се своди само на способност коришћења савремених алата. Она треба да обухвати разумевање начина на који алгоритми функционишу, препознавање ризика по приватност, критичко процењивање информација и одговорно управљање сопственим подацима. Ученици и студенти који разумеју како дигиталне платформе прикупљају и користе њихове податке имају веће могућности да доносе информисане одлуке о сопственом дигиталном понашању.

Анализа регулаторног оквира показује да се заштита приватности све више настоји повезати са управљањем ризицима вештачке интелигенције. GDPR поставља основне принципе обраде личних података, док EU AI Act уводи свеобухватнији приступ регулисању система вештачке интелигенције према степену ризика који могу представљати за појединце и друштво

(European Parliament & Council of the European Union, 2016, 2024). Ипак, постојање регулативе само по себи није довољно. Њена ефикасност зависи од примене у пракси, способности институција да надзиру алгоритамске системе и спремности организација да принципе заштите података интегришу у сам процес развоја и употребе технологије. На основу анализе може се закључити да одговорна примена вештачке интелигенције захтева истовремено деловање на више нивоа. Техничке мере заштите података морају бити праћене правним механизмима, етичким принципима, транспарентношћу алгоритама и људским надзором. Посебно је важно применити принцип „приватности по дизајну”, према којем се заштита личних података узима у обзир већ приликом пројектовања система. У медијима то подразумева већу транспарентност алгоритамске персонализације, док у образовању захтева посебно пажљиво управљање подацима ученика и студената.

Добијени теоријско-аналитички увиди потврђују да се технолошки напредак и заштита приватности не морају посматрати као супротстављени циљеви. Напротив, одговорно пројектовани и регулисани AI системи могу омогућити коришћење предности вештачке интелигенције уз смањење ризика по основна права. Кључни предуслов за то јесте успостављање равнотеже између иновација, економске и друштвене користи, с једне стране, и приватности, аутономије и достојанства појединца, с друге стране.

ЗАКЉУЧАК

Развој вештачке интелигенције и све интензивнија примена алгоритамских система представљају једну од најзначајнијих технолошких промена савременог дигиталног друштва. Њихова примена омогућава ефикаснију обраду великих количина података, персонализацију садржаја и услуга и унапређење различитих друштвених процеса, али истовремено отвара значајна питања у погледу заштите приватности и основних људских права. Анализа је показала да најзначајнији ризици по приватност произилазе из све већег обима прикупљања и обраде личних података, алгоритамског профилисања, аутоматизованог доношења одлука и ограничене транспарентности сложених алгоритамских система. Посебан проблем представља могућност повезивања различитих извора података, чиме се могу формирати детаљни профили појединаца и изводити закључци о њиховом понашању, интересовањима и карактеристикама. Медији и друштвене мреже представљају посебно значајно подручје ових изазова, јер алгоритми све више утичу на избор и персонализацију садржаја који грађани добијају. Истовремено, примена вештачке интелигенције у образовању доноси могућности за персонализовано учење и унапређење наставног процеса, али захтева пажљиво управљање подацима ученика и студената. Посебну заштиту потребно је обезбедити када је реч о деци и младима, чији се подаци могу користити за креирање дугорочних дигиталних профила. Заштита приватности зато не може бити заснована искључиво на техничким мерама, већ захтева повезивање правних, етичких, организационих и образовних механизма. Регулаторни оквири, као што су GDPR и EU AI Act, представљају важне инструменте за управљање ризицима, али њихова ефикасност зависи од доследне примене и развоја институционалних механизма надзора. Принципи транспарентности, одговорности, људског надзора и „приватности по дизајну” треба да постану саставни део развоја и употребе AI система. Посебно важну улогу има образовање, јер заштита приватности у дигиталном добу подразумева и способност грађана да разумеју како алгоритми функционишу и на који начин се њихови подаци користе. Развој дигиталне и AI писмености ученика, студената и наставника

може допринети одговорнијем коришћењу вештачке интелигенције и већој свести о ризицима по приватност. На основу свега наведеног може се закључити да технолошки напредак и заштита приватности не представљају нужно супротстављене циљеве. Одговорна примена вештачке интелигенције могућа је уколико се технолошки развој прати одговарајућом регулативом, етичким стандардима, институционалним надзором и континуираним образовањем корисника. Будућа истраживања требало би усмерити на праћење практичне примене нових регулаторних решења, развој транспарентнијих алгоритамских система и испитивање ефеката примене AI на приватност, нарочито у медијском и образовном окружењу.

РЕФЕРЕНЦЕ

European Commission. (2019). *Ethics guidelines for trustworthy AI*. Publications Office of the European Union.

European Commission. (2022). *Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators*. Publications Office of the European Union.

European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, 1–88.

European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. *Official Journal of the European Union*.

Helberger, N., Pierson, J., & Poell, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information Society*, 34(1), 1–14. <https://doi.org/10.1080/01972243.2017.1391913>.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, 389–399. <https://doi.org/10.1038/s42256-019-0088-2>.

Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, 20(1), 14–29. <https://doi.org/10.1080/1369118X.2016.1154087>.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. <https://doi.org/10.1177/2053951716679679>.

Napoli, P. M. (2019). *Social media and the public interest: Media regulation in the disinformation age*. Columbia University Press.

Republic of Serbia. (2018). *Law on personal data protection*. *Official Gazette of the Republic of Serbia*, No. 87/2018.

Republic of Serbia. (2020). *Strategy for the development of artificial intelligence in the Republic of Serbia for the period 2020–2025*. Government of the Republic of Serbia.

UNESCO. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.

UNESCO. (2023). *Guidance for generative AI in education and research*. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000386693>.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 2019(2), 494–620. <https://doi.org/10.7916/cblr.v2019i2.3424>.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ixp005>.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

CIP - Каталогизација у публикацији
Библиотеке Матице српске, Нови Сад
930.85(497.113)

КАРЛОВАЧКИ лист 021 / главни и одговорни уредник Бранислав Санчанин.
- Год. 1, бр. 1 (2022)- . - Сремски Карловци : Центар за културу, едукацију и
медије "Академац", 2022- (Београд : PROOF). - 30 cm
Годишње.

ISSN 2956-0217 = Карловачки лист 021
COBISS.SR-ID 79126025

