УДК 351.86(497.11)"20"
DOI: 10.5937/pnb31-60690
Прегледни рад

Политика националне безбедности
Година XVII вол. 31
Бр. 1/2026
стр. 197-217

Богдана Стјепановић*

Институт за политичке студије, Београд, Република Србија

Срђана Ђурашевић**

Факултет за међународну политику и безбедност, Универзитет „Унион – Никола Тесла”, Београд, Република Србија

ИНДИРЕКТНЕ ИМПЛИКАЦИЈЕ ШЕРЕНТИНГА НА НАЦИОНАЛНУ БЕЗБЕДНОСТ РЕПУБЛИКЕ СРБИЈЕ

Сажетак

Глобални феномен „шерентинга”, дефинисан као екстензивно дељење личних података малолетних лица на интернету од стране родитеља, представља комплексну индиректну претњу по националну безбедност. Иако су мотиви за шерентинг доминантно некритички и вођени тренутним друштвеним трендовима, крајњи исход је креирање дигиталног отиска за будуће генерације, чиме се дугорочно компромитује њихов информациони суверенитет. У Републици Србији дигитални ризици су додатно наглашени услед неусклађености између високе стопе дигиталне ангажованости младих и дефицита знања родитеља о аспектима информационе безбедности. Док су директне последице, попут крађе идентитета, детаљно документоване, овај рад аргументује да кумулативни подаци проистекли из шерентинга служе као стратешки обавештајни ресурс за државне и недржавне актере. Системско прикупљање ових информација омогућава софистицирано психолошко профилисање, екстензиван надзор и циљане операције утицаја, које могу компромитовати кључно државно особље и

* Имејл адреса: bogdana.stjepanovic@ips.ac.rs; ORCID: 0000-0002-9504-473X.
** Имејл адреса: srdjanadjurasevic98@gmail.com; ORCID: 0009-0009-0141-7442.

нарушити друштвену кохезију. Постојеће рањивости националног сајбер-безбедносног система, праћене изазовима у имплементацији легислативе, стварају амбијент погодан за експлоатацију података. Сузбијање ових претњи захтева координисан стратешки приступ који интегрише унапређење правних оквира, техничку заштиту критичне инфраструктуре и системску дигиталну едукацију. Ублажавање ризика проистеклих из шерентинга није само мера заштите деце, већ и неопходан корак у очувању националне безбедности.

Кључне речи: шерентинг, национална безбедност, информациони рат, заштита података о личности, стратешка отпорност.

УВОД

Термин „шерентинг" (настао спајањем енглеских речи *sharing* – дељење и *parenting* – родитељство) односи се на широко распрострањену праксу родитеља који путем интернета деле информације, фотографије, приче и видео-записе о својој деци, често у претераној мери (Stephenson et al. 2024). Ова појава попримила је глобалне размере и постала општеприхваћен друштвени феномен. Истраживања указују на то да се велика већина родитеља који користе друштвене мреже активно бави шерентингом (чак 82% родитеља обухваћених анкетом из 2020. године потврдило је овакво понашање) (Auxier et al. 2020). У савременом добу, дигитално присуство детета често почиње већ током пренаталног периода дељењем снимака са ултразвука, због чега просечно петогодишње дете иза себе већ има и до хиљаду јавно доступних фотографија (Gatto, Corsello, and Ferrara 2024).

Мотивација за овакво поступање родитеља је комплексна и заснована на бројним факторима, који обухватају како личне потребе, тако и спољашње притиске. Унутрашњи покретачи примарно су везани за емоционално задовољство, жељу за чувањем успомена и јавно истицање дечијих успеха. Насупрот томе, спољашњи подстицаји долазе кроз тежњу за социјалном валидацијом унутар онлајн заједница, притисак вршњака, као и кроз „менаџмент утиска" (настојање да се пројектује специфична слика о родитељству). Такође, значајан фактор представља и

економска корист од креирања „инфлуенсерског" садржаја (Motevalli et al. 2025, 3).

Друштвене мреже су самим својим дизајном пројектоване тако да активно подстичу шерентинг, користећи специфичне економске моделе за сопствени раст. Алгоритми приоритет дају садржају на којем су деца јер такве објаве генеришу далеко већи број лајкова и коментара, што поједини родитељи директно користе за остваривање зараде (Serna 2024, 396). Овај процес ствара затворени круг, што је већа интеракција публике, то су родитељи мотивисанији да деле још приватније податке, чиме се ствара континуиран подстицај за откривање осетљивих информација. На тај начин, потреба тржишта за специфичним садржајем често надјача родитељски опрез, што резултира непрекидним приливом интимних података о деци у јавној сфери. Системи за алгоритамско појачавање видљивости стварају енормне количине података који далеко превазилазе појединачне одлуке појединца. Овако повећана доступност информација заправо проширује базе података које страни актери могу искористити за различите облике експлоатације, чиме се индиректно угрожава национална безбедност.

Република Србија се суочава са специфичним изазовом, висок степен усвајања дигиталних технологија међу младима праћен је ниским нивоом свести о потреби заштите и адекватним превентивним мерама. Деца и млади у Србији показују изузетну дигиталну активност – чак 86% популације узраста од девет до 17 година свакодневно користи паметне телефоне. Посебно је забрињавајуће што значајан удео млађе деце (41% у узрасту девет до десет година и 72% у узрасту једанаест до дванаест година) поседује профиле на друштвеним мрежама или гејминг платформама, иако је прописана старосна граница за већину њих 13 година (Kuzmanović i dr. 2019, 11). Интензивно дигитално присуство деце у Србији не прати сразмерна информисаност родитеља. Многи родитељи не поседују знања и вештине неопходне за безбедно управљање онлајн активностима своје деце. Технички алати, попут „родитељске контроле", користе се у изузетно малој мери – мање од петине ученика потврђује њихову примену, што је знатно испод просека других земаља (Kuzmanović i dr. 2019, 13).

Иако Србија поседује правни оквир, првенствено у виду Закона о заштити података о личности – ЗЗЛП (Zakon o zaštiti podataka o ličnosti [ZZPL] 2018), који је усклађен са ГДПР регулативом (*General Data Protection Regulation – GDPR*), као и државне механизме попут Националног контакт центра за безбедност деце на интернету (European Union 2025), у пракси је уочљив јаз између прописа и њихове имплементације. Низак ниво свести родитеља сугерише да институционалне мере још увек нису довеле до суштинске промене понашања на нивоу породице. Проблем није само у законима, већ и у изазовима њиховог спровођења, недовољном разумевању јавности и својеврсном културолошком отпору према дигиталној безбедности. Управо тај јаз чини податке деце у Србији рањивим. Нерегулисан проток информација омогућава различитим субјектима, укључујући и стране противнике, да прикупљене податке обједине и злоупотребе, што индиректно угрожава безбедност државе.

МЕХАНИЗМИ ДИГИТАЛНОГ ПРОФИЛИСАЊА И НАДЗОРА

Индустрија оглашивачке технологије (*adtech*) и посредници у трговини подацима (*data brokers*) одржавају комплексну мрежу која акумулира екстензивне количине личних података путем технологија за праћење, укључујући дигиталне колачиће (Archbold et al. 2021, 857). Овај процес обухвата све врсте осетљивих информација – од демографских карактеристика попут религије и расе, преко политичких опредељења и здравственог стања, па све до прецизних података о тренутној локацији корисника (Sherman 2024). Као и у готово свим другим сегментима, деца су овде изложена највећем ризику. Због свог узраста, она не разумеју у потпуности комплексност дигиталног окружења и немају капацитет да доносе информисане одлуке о заштити сопствене приватности (Archbold et al. 2021, 858).

Пракса шерентинга додаје екстензивне податке у комерцијалне базе без знања родитеља, пружајући детаљне информације о деци од њихових најранијих година. Те базе садрже податке за личну идентификацију (*Personally Identifiable Information – PII*), информације о локацији и дневним рутинама, породичне односе, па чак и осетљиве биометријске податке

попут отисака прстију или дланова (Stephenson et al. 2024). Овако велика збирка података о деци испоставља се као кључна за развој напреднијих капацитета вештачке интелигенције (*artificial intelligence – AI*) и алгоритама. Софтвер за препознавање лица се, на пример, може обучавати на обимним колекцијама дечјих слика, што омогућава дугорочну идентификацију и праћење појединаца како старе. Надаље, сами AI алати постају „оружје" за различите облике експлоатације, укључујући креирање или измену слика и симулацију експлицитних разговора са децом (Missingkids 2024).

Комерцијална агрегација дечјих података, поспешена шерентингом, генерише доступан и стратешки релевантан обавештајни ресурс за стране противнике. Непријатељски државни актери могу приступити овим колекцијама кроз тржишне трансакције или легалне методе прикупљања, чиме се елиминише потреба за комплексним сајбер-упадима (Office of Public Affairs 2025). Оваква инструментализација података омогућава изградњу еволуирајућих профила појединаца од детињства до одраслог доба, пружајући могућности за дугорочну експлоатацију података у сврхе шпијунаже, уцене или операција утицаја. За Републику Србију то значи да би значајан део будуће радне снаге, војног особља и државних лидера могао бити превентивно профилисан од стране спољних ентитета, што директно нарушава националну отпорност и компликује контраобавештајну заштиту.

Овај обавештајни капитал представља оперативну основу за ОСИНТ (*Open Source Intelligence – OSINT*) и СОЦМИНТ (*Social Media Intelligence – SOCMINT*) стратегије. Интеграцијом различитих података са друштвених мрежа, страни актери конструишу софистициране психолошке досијее који откривају интимне рањивости појединца (Stephenson et al. 2024). Обавештајни рад на друштвеним мрежама СОЦМИНТ, као подскуп обавештајног рада из отворених извора ОСИНТ, омогућава прикупљање и анализу информација са платформи као што су Фејсбук (*Facebook*), Инстаграм (*Instagram*) и Тикток (*TikTok*) (OSINT 2025). Тако генерисани подаци помажу у изградњи комплетних психолошких профила који разоткривају лична уверења, емоционалне реакције и моделе пријема информација (Stegen 2025, 248). Наведени профили имају стратешку примену у регрутовању људских извора, дипломатским преговорима и циљаним операцијама утицаја (248). Потпуно познавање

психолошког профила омогућава технике манипулације које разоткривају скривене рањивости проистекле из садржаја дељеног у детињству. Путем анализе података из шерентинга, противници могу идентификовати специфичне слабости, попут породичне динамике, здравствених проблема или психолошких траума (Stephenson et al. 2024). Такве информације омогућавају развој персонализованих тактика социјалног инжењеринга, што представља претњу демократским процесима и националној кохезији. Стране службе изграђују досијее који прате емоције и везе појединца од рођења, користећи емоционалне окидаче за регрутацију или уцену будућих носилаца осетљивих функција пре него што они уопште ступе на дужност.

Поред непосредне манипулације, дигитални трагови омогућавају форму „трајног надзора" који може трајати деценијама. Са напретком предиктивне аналитике, почетне објаве родитеља еволуирају у алат за социјално сортирање и мониторинг будућих генерација (Stephenson et al. 2024). Компаније за дигитални надзор (*dataveillance*) креирају профиле који се дистрибуирају агенцијама за запошљавање и образовним институцијама, користећи алгоритме за предвиђање о будућем понашању и лојалности појединца (Haley 2020, 1010). Расте забринутост и због државног надзора који обједињује податке са мрежа, паметних уређаја и медицинских картона, често потпомогнутог законима који захтевају локално складиштење података ради лакшег приступа служби безбедности (Feldstein 2020, 2). Свеобухватно дигитално каталогизовање националних људских ресурса омогућава противницима да „култивишу" појединце годинама пре него што они постану стратешки релевантни, чиме се компромитује целокупан систем институција и међуљудска интеракција као константна тачка потенцијалне експлоатације.

ГЕОПОЛИТИЧКИ УТИЦАЈ И ИНФОРМАЦИОНИ РАТ

Осетљиви лични подаци, који укључују прецизне геолокацијске параметре (нпр. са војних објеката) или интимне појединости, могу бити инструментализовани од стране страних противника у сврху присиле или уцене појединаца са приступом поверљивим националним информацијама (Sherman 2024).

Шерентинг ненамерно открива детаље о породичним рутинама и личним рањивостима деце, чиме ови подаци постају доступни за обавештајно прикупљање. Обиље информација о емоционалним стањима и обрасцима понашања омогућава спољним актерима да разумеју психолошке профиле појединаца, што је кључна основа за спровођење операција утицаја (Stegen 2025, 248). Ови подаци се користе за конструисање високоперсонализованих покушаја „фишинга" (*phishing*)[1] и других метода дигиталне обмане усмерених на родитеље који заузимају стратешке позиције у владином сектору, војсци или критичној инфраструктури.

Екстензивно обелодањивање породичних појединости ствара оптимално окружење за операције прикупљања обавештајних података путем људских извора (*human intelligence – HUMINT*). Ови подаци олакшавају идентификацију појединаца са породичним рањивостима (нпр. здравствени проблеми или компромитујући детаљи из прошлости), финансијским притисцима или личним тајнама погодним за уцену и регрутовање. Ризик од „инсајдерских претњи" се увећава када су мета припадници војске и обавештајних служби, јер њихови приватни животи постају рањиве тачке кроз које страни актери врше притисак. Неформално дељење садржаја на мрежи директно подрива безбедност државе компромитовањем интегритета и лојалности кључног особља, чиме се дугорочно слабе одбрамбени капацитети државе.

Психолошки подаци прикупљени путем шерентинга омогућавају креирање ефикасних пропагандних кампања и дезинформација (Stegen 2025, 252). Ова појава се може подвести под фазу синтетичке пропаганде, коју карактерише употреба алата вештачке интелигенције за конструисање уверљивог, али лажног садржаја (Kazić 2025, 108). У ширем безбедносном контексту, овакав вид деловања постаје интегрални део хибридног ратовања, где се кроз синергију насилних и ненасилних садржаја настоји дестабилизовати вредносни темељ нападнуте државе (Đorđević і Miljković 2025, 169). Разумевањем психолошких предрасуда унутар популације, страни противници могу обликовати наративе који

[1] Фишинг је врста интернет преваре којом нападачи, лажно се представљајући као поверљива институција или особа (банке, друштвене мреже, сервиси), обмањују кориснике како би украли осетљиве податке попут лозинки, бројева кредитних картица или инсталирали малициозни софтвер (Microsoft 2026).

подривају поверење у институције. Психолошка штета проистекла из шерентинга постаје стратешко оружје у операцијама страног утицаја, где се користи за интензивирање унутрашњих друштвених конфликата (Stephenson et al. 2024).

Психолошке информације, друштвени обрасци и унутрашњи конфликти становништва (укључујући и младе), садржани у подацима проистеклим из шерентинга, пружају страним противницима софистицирана средства за успешно извођење операција информационог ратовања. То може укључивати микроциљану пропаганду усмерену на специфичне демографске групе, продубљивање постојећих друштвених подела (нпр. међугенерацијски конфликти око приватности, права родитеља наспрам права детета) или систематско подривање поверења јавности у владу, медије и демократске процесе. За државу попут Србије, која пролази кроз демократске реформе и тежи ка приступању ЕУ, овакве спољне манипулације засноване на лако доступним личним подацима представљају значајну претњу по демократску стабилност, друштвену кохезију и националну безбедност (Eurochild 2025). Страни актери могу користити овај метод за притајено обликовање ставова јавности и интензивирање друштвених сукоба уз истовремено урушавање поверења у националне институције, чак и без директних сајбер напада на инфраструктуру. Постепено слабљење друштвеног јединства, у комбинацији са ослабљеним демократским институцијама, ствара велику индиректну претњу по државну безбедност. У геополитички осетљивом региону попут Балкана, где се историјске тензије лако могу поново распламсати, овај облик информационог рата заснован на подацима представља посебно акутан ризик за будућу стабилност и безбедност Србије.

КОНТЕКСТУАЛНЕ РАЊИВОСТИ И ИЗАЗОВИ У УПРАВЉАЊУ ПОДАЦИМА У РЕПУБЛИЦИ СРБИЈИ

Иако су поменути ризици глобални по свом обиму, они попримају специфичну хитност у Републици Србији. Јединствени пресек високе дигиталне ангажованости младих и мањка „дигиталне хигијене" код родитеља ствара плодно тло за експлоатацију. Док грађани покушавају да се заштите од спољних

претњи, домаћа правна и безбедносна инфраструктура и даље се бори са значајним празнинама у заштити.

Устав Републике Србије садржи одредбе о заштити приватности (чл. 41) и података о личности (чл. 42) (Ustav Republike Srbije, čl. 41 i 42, 2006). Ове одредбе представљају оквире за прикупљање података који штите личне информације од злоупотребе, осим у случајевима неопходним за вођење кривичног поступка или заштиту националне безбедности. Србија од 2019. године примењује ЗЗПЛ, који је у великој мери усклађен са Општом уредбом ЕУ о заштити података (*General Data Protection Regulation – GDPR*) (Đerić, Radović, and Petrović 2025). Закон о заштити података о личности захтева пристанак корисника пре обраде података, али намеће додатне услове за пристанак и даје субјектима право да захтевају потпуно уклањање информација („право на заборав"). За малолетнике млађе од 14 година, неопходан је пристанак родитеља или старатеља (Letslaw 2024).

Повереник за информације од јавног значаја и заштиту података о личности је примарни регулатор за заштиту података у Србији, са истражним, корективним и саветодавним овлашћењима сличним надзорним телима у оквиру ГДПР. Међутим, иако Повереник спроводи инспекцијске надзоре (731 у 2023. години) и изриче опомене (51 у 2023. години), број покренутих прекршајних поступака (свега десет у 2023. години) делује недовољно с обзиром на обим потенцијалних кршења. Повереник се такође суочава са правним изазовима, укључујући тужбе Министарства унутрашњих послова поводом налога за брисање података (Đerić, Radović, and Petrović 2025).

Упркос међународним инструментима за људска права, као што су Конвенција УН о правима детета (чл. 16 и 19), која штити приватност деце, Конвенција о заштити лица у односу на аутоматску обраду личних података (Zakon o potvrđivanju konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka [ZPKZL] 2010) и Конвенција Савета Европе о заштити деце од сексуалног искоришћавања и сексуалне злоупотребе (Ланзароте конвенција), која криминализује онлајн дечју порнографију и „груминг" (*grooming*)[2], Србији тренутно недостаје свеобухватан

[2] Груминг је назив за процес којим најчешће почиње сексуално злостављање деце, а преводи се као „врбовање" или „намамљивање". То је процес у којем се

Закон о правима детета. Уместо тога, правне одредбе које се тичу деце део су различитих националних закона (образовање, здравство, социјална заштита итд.). Поред тога, главно надзорно тело, Савет за права детета, остаје неактиван упркос поновном оснивању у марту 2023. године (Eurochild 2023).

Тренутни правни систем пружа опсежну општу заштиту података, али не успева да успостави специфичне и робусне стандарде који би заштитили дигиталну приватност деце у ситуацијама када родитељи деле њихове податке. Такође, механизмима за спровођење закона недостаје капацитет да се изборе са масовношћу праксе шерентинга. Ово ствара осетљиво окружење које омогућава страним противницима бројне прилике за експлоатацију прикупљених осетљивих података о деци.

Република Србија поседује сајбер-безбедносни систем који се континуирано развија, али се суочава са изазовима који произилазе како из спољних претњи, тако и из системских сложености у управљању подацима. Званични национални подаци указују на структурну рањивост која се огледа у драматичном порасту потрошње мобилног интернета и дигиталне повезаности, при чему саобраћај мобилног интернета у Србији бележи експоненцијални раст (RATEL 2024, 22). Иако домаће законодавство пружа оквир за борбу против високотехнолошког криминала, ефикасност његове примене често је предмет академских дебата. Посебно се истиче забринутост у вези са оперативним капацитетима Националног ЦЕРТ (*Computer Emergency Response Team – CERT*) да одговори на масовну експлоатацију података која је олакшана шерентингом (Dennis 2024). Овај јаз између законодавног оквира и оперативне стварности ствара стратешки простор који страни актери користе за прикупљање психолошких података и спровођење софистицираних операција утицаја (Stegen 2025, 248). Поред тога, питање дигиталне приватности у Србији нераскидиво је повезано са употребом напредних форензичких и надзорних технологија. Стручне анализе и извештаји организација цивилног друштва све чешће отварају питања о адекватности надзорних механизама који регулишу примену софистицираних алата за прикупљање података

потенцијални сексуални злостављач спријатељује с дететом и задобија његово поверење како би покушао да га укључи у (сексуалне) злостављачке активности (Nacionalni kontakt centar za bezbednost dece na internetu 2023).

(Ristić 2023, 17–19; Amnesty 2024). Са становишта националне безбедности, примарни изазов не лежи само у поседовању ових капацитета, већ у „дефициту поверења" који њихова нетранспарентна употреба може изазвати код грађана. Када јавност перципира да институције не поступају са подацима на потпуно јасан и контролисан начин, долази до пада поверења, што директно утиче на спремност појединаца да усвоје основне мере „дигиталне хигијене" и безбедносне протоколе (Ristić 2023, 15). Додатне компликације у овој области узрокују документовани пропусти у великим јавним базама података, који наглашавају техничке и системске слабости националне дигиталне инфраструктуре. Концентрација осетљивих података грађана у објектима као што је Државни дата центар, иако усмерена ка њиховој заштити, истовремено ствара значајну мету за потенцијалну експлоатацију и неовлашћени приступ (10). У таквим околностима, ерозија поверења јавности прераста у стратешку рањивост. Становништво које нема поверења према домаћем систему управљања подацима постаје подложније страним операцијама утицаја и експлоатацији података од стране спољних актера. Из тог разлога, отпорност безбедносног система Србије директно зависи од јачања транспарентности дигиталног надзора и успостављања робуснијих механизама за заштиту података о личности.

Кроз бројне домаће и међународне иницијативе Република Србија показује посвећеност заштити деце на интернету и подизању свести о дигиталним ризицима. Национални контакт центар за безбедност деце на интернету служи као кључна национална иницијатива од 2017. године, пружајући саветодавну подршку, прослеђујући случајеве злоупотребе надлежним институцијама и спроводећи превентивне едукације у школама (European Union 2025). Организација УНИЦЕФ (*United Nations International Children's Emergency Fund – UNICEF*) Србија такође активно сарађује са државним и приватним сектором на изградњи заштићеног дигиталног простора за децу (Unicef Serbia 2017). Ови програми укључују платформе попут „Паметно и безбедно", кроз које је у 2023. години обављено 120 едукативних предавања широм Србије, обухвативши 7.800 ученика, 1.000 родитеља и 300 наставника (European Union 2025).

Србија је такође потписница Будимпештанске конвенције о сајбер криминалу и Ланзароте конвенције, те сарађује са

Интерполом (*Interpol*) на пројектима као што је Спречавање штетног утицаја (*Disrupting Harm*), усмереним на сузбијање онлајн сексуалне експлоатације деце (OSINT 2025). Упркос похвалним напорима, празнине и даље постоје. Свест јавности о сајбер безбедности се поправља, али је и даље недовољна (Dennis 2024). Многи родитељи немају довољно знања о онлајн претњама и ретко користе техничке контроле. Истраживања указују на то да деца често помажу родитељима у дигиталним задацима, што открива дефицит знања код одраслих који тренутне иницијативе можда не решавају ефикасно (Kuzmanović i dr. 2019).

Иако иницијативе за превенцију шерентинга у Србији показују снажну намеру и широк обухват, стални изазови у едукацији родитеља и слаба примена техничких мера заштите указују на то да ови програми још увек нису достигли размеру потребну за промену распрострањеног понашања и минимизирање ризика од излагања података. Програм за заштиту опште безбедност на интернету не бави се софистицираним методама које напредни актери користе за прикупљање и злоупотребу података које служи као оружје у даљим усмереним операцијама. То указује на то да тренутни приступ, упркос позитивним сигналима, делује неадекватно за истовремено сузбијање масовне праксе шерентинга и софистицираних метода експлоатације података од стране страних противника. Реч је о трци с временом у којој је прикупљање података брже од раста свести јавности. То практично значи да значајан део српског друштва остаје изложен индиректним ризицима по националну безбедност, јер њихови подаци отичу у отворене изворе (*open-source*) где постају лаки плен за експлоатацију.

СТРАТЕШКЕ ПРЕПОРУКЕ ЗА ЈАЧАЊЕ НАЦИОНАЛНЕ ОТПОРНОСТИ

Како би се на адекватан начин одговорило на индиректне импликације шерентинга по националну безбедност Републике Србије, неопходан је свеобухватан и координисан стратешки приступ. Ове стратешке препоруке фокусиране су на снажење правних оквира, унапређење сајбер заштите, промоцију дигиталне писмености и подстицање међународне сарадње.

Доношење посебног Закона о правима детета требало би да представља приоритет Србије у домену заштите дечјих права. Неопходно је да овај нови законски акт обухвати питања дигиталне приватности, шерентинга и пристанка детета кроз јединствене и свеобухватне правне одредбе, уместо кроз фрагментирана законска решења. Закон би требало да садржи јасне прописе о „праву на заборав", које би деца могла да остваре након стицања пунолетства, чиме би им се омогућило да захтевају брисање садржаја који су објавили родитељи или трећа лица. Такође, Повереник за информације од јавног значаја и заштиту података о личности мора добити већа средства, напредније техничке алате и специфична овлашћења за вођење истрага и санкционисање прекршаја у случајевима шерентинга и експлоатације података о деци (Đerić, Radović, and Petrović 2025). Неопходно је да ово тело прецизно дефинише своје надлежности у вези са родитељским дељењем података и обезбеди ефикасно поступање по свим примљеним притужбама.

Правни систем захтева програме континуиране едукације фокусиране на дигиталну приватност, шерентинг, као и на питања агрегације и експлоатације података у контексту дечјих права и националне безбедности, намењене припадницима полиције, судијама и тужиоцима (Gatto, Corsello, and Ferrara 2024). Ово би омогућило суптилнији и ефикаснији правни одговор на савремене дигиталне претње. Поред тога, потребно је да Влада Србије интензивира напоре на усклађивању стандарда заштите података и дигиталних услуга са оквирима Европске уније, нарочито са Актом о дигиталним услугама (*Digital Services Act – DSA*). Овом мером Србија би остварила бољи надзор над онлајн платформама које послују на њеној територији, као и ефикасније механизме за сузбијање штетног садржаја и злоупотребе података.

Упоредо са правним реформама, неопходно је утврдити критичну техничку инфраструктуру. Органи задужени за националну безбедност требало би да имплементирају ригорозне мере сајбер заштите како би осигурали виталне државне базе података и основне услуге, у оквиру иницијативе за одбрану критичне инфраструктуре. Заштита ових система постаје суштинска јер би хакери могли повезати украдене податке са информацијама прикупљеним путем шерентинга ради креирања комплексних профила појединаца (Dennis 2024). Примена

принципа „интегрисане заштите података" (*data protection by design*) и „подразумеване заштите података" (*data protection by default*) мора постати обавезна за сваку дигиталну услугу и државни систем. Ово подразумева подстицање минимизације података (прикупљање само неопходних информација) уз примену снажне енкрипције и других безбедносних мера. Поред тога, потребно је развити оперативне планове који би спречили посреднике у трговини подацима (*data brokers*) да продају информације о грађанима Србије страним противницима (Sherman 2024). Потребно је да држава успостави строге процедуре за заштиту јавних база података са информацијама о грађанима од неовлашћеног приступа. Свако цурење података из државних регистара које се подудара са информацијама из шерентинга омогућава стварање детаљних профила које непријатељски ентитети могу лако злоупотребити.

Дугорочни имунитет друштва зависи од системског заокрета у области дигиталне писмености и образовања. У том циљу неопходно је спровести кампање за подизање јавне свести које би јасно указале на то како шерентинг компромитује националну безбедност. Образовни садржаји треба да представе примере из стварног света и користе ефектан приступ кроз наратив (*storytelling*), како би објаснили на који начин се рутинско дељење садржаја претвара у опасно коришћење података као оружја (*weaponization of data*) и постаје трајна безбедносна рањивост. Акценат треба ставити на колективну безбедност нације и дугорочне последице по будућност деце. Поред тога, треба увести обавезну дигиталну писменост у образовни систем, од раног детињства до адолесценције. Образовни програм треба да обучи ученике критичком промишљању о онлајн садржају, управљању приватношћу и разумевању трајног дигиталног отиска.

Паралелно са системским мерама, неопходно је информационо оснажити родитеље кроз практичне и културолошки прилагођене ресурсе који омогућавају непосредну примену стратегија заштите приватности, попут техника замућивања лица или строге контроле метаподатака PII. У овом контексту, јавне личности и инфлуенсери у Србији носе посебну друштвену одговорност да својим примером предводе промоцију етичког шерентинга и дигиталне дискреције (European Union 2025). На макроплану, национална безбедност Србије мора бити подупрта

интензивном прекограничном сарадњом. То подразумева јачање партнерстава са институцијама попут Европске уније, УНИЦЕФ, Интерпола и Европола (*Europol*), првенствено у оквиру размене оперативних обавештајних података о софистицираним облицима дигиталне експлоатације деце. Да би се ови напори материјализовали, неопходно је обезбедити континуирану подршку развоју техничких капацитета домаћих органа реда и обавештајних агенција, са посебним фокусом на унапређење дигиталне форензике и експертизе у областима ОСИНТ и СОЦМИНТ аналитике (Conti et al. 2024). Напослетку, Влада Србије треба да се на међународној сцени позиционира као заговорник глобалних стандарда за заштиту дигиталних права деце. Овакво стратешко деловање има за циљ не само заштиту појединаца, већ и системско ограничавање неконтролисане експлоатације података од стране комерцијалних и државних актера, чиме се суштински чува информациони суверенитет и будућност нације у информационом добу.

ЗАКЉУЧАК

Шерентинг данас превазилази оквире приватне породичне праксе и постаје кључни фактор у домену националне безбедности Републике Србије. Нехотично креирање трајних дигиталних идентитета деце, уз системску агрегацију осетљивих података од стране комерцијалних ентитета, претвара личне информације у стратешке обавештајне ресурсе. Спољни актери ове изворе могу користити за психолошко профилисање, дугорочни надзор и операције утицаја, чиме се потенцијално угрожава интегритет кључног особља и слаби друштвена кохезија.

Специфичност дигиталног окружења у Србији огледа се у несразмери између интензивног коришћења интернета код младих и дефицита дигиталне писмености код родитеља. Иако је домаћи правни оквир у великој мери усклађен са међународним стандардима, ефикасност сузбијања негативних ефеката шерентинга ограничена је одсуством специфичне легислативе о правима детета, као и изазовима у имплементацији постојећих прописа. У том контексту, питање транспарентности државних механизама надзора постаје кључно за изградњу јавног поверења. Дефицит тог поверења не представља само унутрашњи друштвени проблем већ и системску рањивост која слаби друштвену

отпорност, чинећи становништво подложнијим софистицираним спољним притисцима и манипулацији подацима.

Суочавање са овом појавом није искључиво питање индивидуалне заштите приватности, већ императив националне безбедности. Изградња друштвене отпорности захтева проактиван приступ који обједињује јачање правних механизама, унапређење државног управљања подацима и системску дигиталну едукацију. Заштита дигиталне будућности најмлађих грађана суштински је предуслов за очување дугорочне стабилности и интегритета Републике Србије у глобалном информационом поретку заснованом на подацима.

РЕФЕРЕНЦЕ

Amnesty International. 2024. "Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists." *Amnesty International*. December 16, 2024. https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/.

Archbold, Lisa, Damian Clifford, Moira Paterson, Megan Richardson, and Normann Witzleb [Archbold et al.]. 2021. "Adtech and Children's Data Rights." *UNSW Law Journal* 44 (3): 857–877.

Auxier, Brooke, Monica Anderson, Andrew Perrin, and Turner, Erica [Auxier et al.]. 2020. "Parenting Children in the Age of Screens." *Pew Research Center*. Last Accessed on January 29, 2026. https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/.

Conti, Maria Giulia, Fabiola Del Parco, Francesca Maria Pulcinelli, Enrica Mancino, Laura Petrarca, Raffaella Nenna, Greta Di Mattia, Luigi Matera, Domenico Paolo La Regina, Enea Bonci, Cinthia Caruso, and Fabio Midulla [Conti et al.]. 2024. "Sharenting: characteristics and awareness of parents publishing sensitive content of their children on online platforms." *Italian Journal of Pediatrics* 50 (1): 135. DOI: 10.1186/s13052-024-01704-y.

Dennis, Gavin. 2024. "Cyber Security in Serbia." *Gavin Denis Cyber Security*. October 30, 2024. https://blog.gavindennis.com/cyber-security-in-serbia/.

Đeric, Vladimir, Katarina Radović, and Lena Petrović. 2025. "Data Protection & Privacy 2025 – Serbia." *Chambers and Partners*. Last Updated March 11, 2025. https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/serbia/trends-and-developments/O20227.

Đorđević, Marko, i Milan Miljković. 2025. „Povezanost hibridnog ratovanja i savremenog terorizma." *Politika nacionalne bezbednosti* 28 (1): 167–190. DOI: 10.5937/pnb28-57340.

Eurochild. 2023. "Serbia Children's Rights Political will or wont." *Eurochild*. Last Accessed on January 29, 2026. https://eurochild.org/uploads/2024/02/Serbia-Childrens-Rights-Political-will-or-wont.pdf.

Eurochild. 2025. "The rights of children under threat in Serbia." *Eurochild*. April 14, 2025. https://eurochild.org/news/the-rights-of-children-under-threat-in-serbia/.

European Union. 2025. "SIC+ programme: Serbia- National Contact Centre for Children Safety on the Internet/Centre for missing and exploited children." *European Union*. Last Updated July 2025. https://better-internet-for-kids.europa.eu/en/sic/serbia.

Feldstein, Steven. 2020. "State surveillance and implications for children." *UNICEF*. Last accessed on January 29, 2026. https://www.unicef.org/innocenti/media/1136/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf.

Gatto, Antonio, Antonio Corsello, and Pietro Ferrara. 2024. "Sharenting: hidden pitfalls of a new increasing trend – suggestions on an appropriate use of social media." *Italian journal of pediatrics* 50 (1): 15. DOI: 10.1186/s13052-024-01584-2.

Haley, Keltie. 2020. "Sharenting and the (Potential) Right to Be Forgotten." *Indiana Law Journal* 95 (3): 1005–1026.

Kazić, Tanja. 2025. „Digitalna propaganda i dezinformacije generisane veštačkom inteligencijom: studije slučaja izraelsko-palestinskog sukoba i pada Bašara al-Asada u Siriji." *Politika nacionalne bezbednosti* 28 (1): 101–122. DOI: 10.5937/pnb28-56408.

Kuzmanović, Dobrinka, Zoran Pavlović, Dragan Popadić, i Tijana Milošević [Kuzmanović i dr.]. 2019. „Korišćenje interneta i digitalne tehnologije kod dece i mladih u Srbiji: Rezultati istraživanja „Deca Evrope na internetu". *UNICEF Srbija*. Poslednji pristup 29. januar 2026. https://www.unicef.org/serbia/media/12511/file/koriscenje_interneta_i_digitalne_tehnologije_kod_dece_i_mladih_u_Srbiji.pdf.

Letslaw. 2024. "Children's right to be forgotten on the Internet." *Letslaw*. November 13, 2024. https://letslaw.es/en/children-right-forgotten-internet/.

Microsoft. 2026. „Šta je phishing?" *Microsoft*. Poslednji pristup 11. marta 2026. https://www.microsoft.com/sr-latn-rs/security/business/security-101/what-is-phishing.

Missingkids. 2024. "2024 CyberTipline Report." *Missingkids*. Last Accessed on January 29, 2026. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.

Motevalli, Saeid, Rogayah A. Razak, Richard Peter Bailey, Amalia B. Madihie, Katayoun Mehdinezhadnouri, and Yifei Pan [Motevalli et al.]. 2025. "Parents' Sharenting Behaviours: A Systematic Review of Motivations, Attitudes, Perceptions, and Impression Management Perspectives." *F1000Research*. 2025 14: 448. DOI: 10.12688/f1000research.161540.1.

Nacionalni kontakt centar za bezbednost dece na internetu. 2023. „Lažna onlajn prijateljstva – Grooming." *Nacionalni kontakt centar za bezbednost dece na internetu*. Poslednji pristup 11. marta 2026. https://www.pametnoibezbedno.gov.rs/vest/sr/598/lazna-onlajn-prijateljstva-grooming.php.

Office of Public Affairs. 2025. "Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries." *Office of Public Affairs*. April 11, 2025. https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive.

OSINT. 2025. "OSINT Training Log: Training Serbian Officials to Combat Child Exploitation." *OSINT*. May 2, 2025. https://www.osint.industries/training-log-posts/osint-training-log-training-serbian-officials-to-combat-child-exploitation.

RATEL. 2024. *Overview of the Electronic Communications and Postal Services Market in the Republic of Serbia in 2023*. *RATEL*. Last accessed on January 29, 2026. https://www.ratel.rs/storage/upload/2025/08/PT23---eng---RATEL.pdf.

Ristić, Andrijana. 2023. "Digital Surveillance in Serbia." *Belgrade Centre for Security Policy*. Last accessed on January 29, 2026. https://bezbednost.org/wp-content/uploads/2023/07/digitalni-eng-01.pdf.

Serna, Aranda. 2024. "Social and Legal Risks of Sharenting when Forming a Child's Digital Identity in Social Networks." *Journal*

of Digital Technologies and Law 2 (2): 394–407. DOI: 10.21202/jdtl.2024.20.

Sherman, Justin. 2024. "Tackling Data Brokerage Threats to American National Security." *Lawfaremedia*. November 25, 2024. https://www.lawfaremedia.org/article/tackling-data-brokerage-threats-to-american-national-security.

Stegen, Johanna Isabella. 2025. "Leveraging social media intelligence (SOCMINT) in the African intelligence context." *Journal of Policing, Intelligence and Counter Terrorism* 20 (2): 243–257. DOI: 10.1080/18335330.2025.2465529.

Stephenson, Sophie, Christopher Nathaniel Page, Miranda Wei, Apu Kapadia, and Roesner Franziska [Stephenson et al.]. 2024. "Sharenting on TikTok: Exploring Parental Sharing Behaviors and the Discourse Around Children's Online Privacy." In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI'24)*, 1–17. New York: Association for Computing Machinery (ACM). DOI: 10.1145/3613904.3642447.

Unicef Serbia. 2017. "Make the digital world safer for children – while increasing online access to benefit the most disadvantaged." *Unicef Serbia*. December 12, 2017. https://www.unicef.org/serbia/en/press-releases/make-digital-world-safer-children-while-increasing-online-access-benefit-most.

Ustav Republike Srbije „Službeni glasnik Republike Srbije" br. 98/2006.

Zakon o potvrđivanju konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka [ZPKZL], „Službeni list SRJ - Međunarodni ugovori", br. 1/92, „Službeni list SCG - Međunarodni ugovori", br. 11/2005 - dr. zakon i „Službeni glasnik RS - Međunarodni ugovori", br. 98/2008 - dr. zakon i 12/2010.

Zakon o zaštiti podataka o ličnosti [ZZPL], „Službeni glasnik Republike Srbije" br. 87/2018.

Bogdana Stjepanović[*]
Institute for Political Studies, Belgrade, Republic of Serbia

Srđana Đurašević[**]
Faculty of International Politics and Security,
University "Union – Nikola Tesla", Republic of Serbia

INDIRECT IMPLICATIONS OF SHARENTING ON THE NATIONAL SECURITY OF THE REPUBLIC OF SERBIA

Resume

The global phenomenon of "sharenting", defined as the extensive sharing of minors' personal data on the internet by parents, represents a complex indirect threat to national security. Although the motives for sharenting are predominantly uncritical and driven by current social trends, the outcome is the creation of a digital footprint for future generations, which compromises their long-term information sovereignty. In the Republic of Serbia, digital risks are further amplified by the misalignment between the high rate of digital engagement among youth and the deficit of parental knowledge in information security. While direct consequences, such as identity theft, are well documented, this paper argues that cumulative data resulting from sharenting serve as a strategic intelligence resource for both state and non-state actors. The systemic collection of this information enables sophisticated psychological profiling, extensive surveillance, and targeted influence operations, which can compromise key state personnel and undermine societal cohesion. Existing vulnerabilities in the national cybersecurity system, coupled with challenges in legislative implementation, create an environment vulnerable to data exploitation. Countering these threats requires a coordinated strategic approach that integrates strengthening legal frameworks, technical protection of critical infrastructure, and systemic digital education. Mitigating the risks arising from sharenting

[*] E-mail address: bogdana.stjepanovic@ips.ac.rs; ORCID: 0000-0002-9504-473X.
[**] E-mail address: srdjanadjurasevic98@gmail.com; ORCID: 0009-0009-0141-7442.

is not merely a child protection measure but a necessary step in preserving national security.

Keywords: sharenting, national security, information warfare, personal data protection, strategic resilience.

* Овај рад је примљен 6. августа 2025. године, а прихваћен за штампу на састанку Редакције 27. фебруара 2026. године.