UDC 351.86(497.11)"20"
DOI: 10.5937/pnb31-60690
Review article

Политика националне безбедности
(The Policy of National Security)
Year XVII vol. 31
No. 1/2026
pp. 197-217

Bogdana Stjepanović*

Institute for Political Studies, Belgrade, Republic of Serbia

Srđana Đurašević**

Faculty of International Politics and Security, University "Union – Nikola Tesla", Belgrade, Republic of Serbia

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

(Translation in *Extenso*)

Abstract

The global phenomenon of "sharenting", defined as the extensive online sharing of minors' personal data by parents, represents a complex and indirect threat to national security. Although the motives behind this practice are predominantly uncritical, it results in the construction of permanent digital identities for future generations without their prior consent. In the Republic of Serbia, digital risks are further exacerbated by the disparity between youth's high digital engagement and parents' limited knowledge of information security. While direct consequences, such as identity theft, are well-documented, this paper argues that aggregated data derived from sharenting serves as a strategic intelligence resource for both state and non-state actors. The systemic accumulation of this information facilitates sophisticated psychological

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

profiling, extensive surveillance, and targeted influence operations, potentially compromising key state personnel and undermining social cohesion. Current vulnerabilities in the national cybersecurity system, coupled with legislative implementation challenges, create an environment that is highly conducive to such data exploitation. Addressing 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 is not merely a child protection measure but an essential step in safeguarding national security.

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

INTRODUCTION

The term "sharenting" (a portmanteau of "sharing" and "parenting") refers to the widespread practice of parents sharing online information, photographs, stories, and videos of their children, often to an excessive degree (Stephenson et al. 2024). This phenomenon has reached global proportions, becoming a normalized social practice. Research indicates that the vast majority of parents active on social media engage in sharenting (82% of parents surveyed in 2020 confirmed such behavior) (Auxier et al. 2020). In the modern era, an individual's digital presence often begins in the prenatal period through the sharing of ultrasound images, resulting in the average five-year-old child having as many as one thousand publicly accessible images online (Gatto, Corsello, and Ferrara 2024).

The motivations behind this parent behavior are complex and rooted in multiple factors, including personal needs and external pressures. Internal drivers are primarily linked to emotional satisfaction, the desire to preserve memories, and the public celebration of a child's achievements. On the other hand, external incentives stem from a need for social validation within online communities, peer pressure, and "impression management" – the effort to project a specific image of parenthood. Additionally, economic benefits associated with creating commercial "influencer" content represent a significant factor (Motevalli et al. 2025, 3).

Social media platforms actively encourage sharenting through their design, utilizing economic models to maximize growth. The algorithmic prioritization of content featuring children results in higher engagement rates (likes and comments), which some parents utilize for financial gain (Serna 2024, 396). Sharenting creates a feedback loop that drives parents to share more personal content, increasing their online engagement and creating a continuous incentive to post more vulnerable information. In this way, content demand outpaces parental safety considerations, resulting in an endless stream of sensitive child information entering the public domain. Algorithmic amplification systems generate enormous volumes of data that transcend individual decisions. This increased accessibility of information regarding children expands the datasets available for exploitation by foreign actors, thereby indirectly threatening national security.

The Republic of Serbia faces a specific challenge: a high adoption rate of digital technologies among youth, coupled with low levels of awareness of protection and preventive measures. Children and adolescents in Serbia demonstrate exceptional digital activity, with 86% of the population aged nine to 17 using smartphones daily. Of particular concern is that a significant proportion of younger children (41% aged nine to ten and 72% aged eleven to twelve) maintain profiles on social media or gaming platforms, despite the minimum age requirement of 13 for most services (Kuzmanović et al. 2019, 11). This intensive digital presence is not matched by parental awareness, as many parents lack the skills needed to manage their children's online activities securely. Technical tools, such as "parental controls", are utilized far less frequently than in other countries, with fewer than one-fifth of students confirming their application (Kuzmanović et al. 2019, 13).

Although Serbia possesses a legal framework primarily consisting of the Law on Personal Data Protection (Zakon o zaštiti podataka o ličnosti [ZZPL] 2018), which is aligned with the General Data Protection Regulation (GDPR), and state mechanisms such as the National Contact Center for Safety of Children on the Internet (European Union 2025), a clear gap remains between regulation and implementation. Low parental awareness suggests that institutional measures have yet to result in a fundamental behavioral shift at the

family level. The issue lies not only in the legislation but also in enforcement challenges, insufficient public understanding, and a degree of cultural resistance to digital security. This disparity renders the data of children in Serbia vulnerable. Unregulated information flows allow various entities, including foreign adversaries, to aggregate and misuse such data, ultimately posing an indirect threat to state security.

THE MECHANICS OF DIGITAL PROFILING AND SURVEILLANCE

The advertising technology (*adtech*) industry and data brokers maintain a complex network that accumulates extensive quantities of personal data through tracking technologies, including digital cookies (Archbold et al. 2021, 857). The data collection includes sensitive information such as demographics (e.g., religion, race), political preferences, health information, and precise geolocation data (Sherman 2024). In almost every area, children face a higher risk of being affected because they do not fully understand the digital environment and lack the capability to make informed decisions (Archbold et al. 2021, 858).

The practice of sharenting adds extensive data to the commercial data pool without parents' knowledge while providing detailed information about children from their earliest years. The database contains Personally Identifiable Information (PII), location data, daily routines, family relationships, and sensitive biometric information, including fingerprints and palm photos (Stephenson et al. 2024). A large collection of child data is essential for developing more effective artificial intelligence (AI) capabilities and algorithms. Facial recognition software, for instance, can be trained on the extensive collection of children's images, enabling long-term identification and tracking as individuals age. Furthermore, AI tools themselves are being weaponized for various forms of exploitation, including the creation or alteration of images and the simulation of explicit chats with children (Missingkids 2024).

The commercial aggregation of children's data, catalyzed by sharenting, creates an accessible, strategically relevant intelligence resource for foreign adversaries. Hostile state actors can access

these collections through market transactions or legal collection methods, thereby eliminating the need for complex cyber intrusions (Office of Public Affairs 2025). This weaponization of data enables the construction of evolving individual profiles from childhood to adulthood, offering opportunities for long-term data exploitation in espionage, blackmail, or influence operations. For the Republic of Serbia, this implies that a significant portion of the future workforce, military personnel, and state leaders could be pre-emptively profiled by external entities, directly eroding national resilience and complicating counterintelligence protection.

This intelligence capital serves as an operational foundation for Open Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT) strategies. By integrating diverse data threads from social media, foreign actors construct sophisticated psychological dossiers that reveal an individual's most intimate vulnerabilities (Stephenson et al. 2024). SOCMINT, a subfield of OSINT, facilitates the collection and analysis of information from platforms such as Facebook, Instagram, and TikTok (OSINT 2025). The data generated contribute to the development of comprehensive psychological profiles that reveal personal beliefs, emotional reactions, and information-processing models (Stegen 2025, 248). These profiles have strategic applications in human source recruitment, diplomatic negotiations, and targeted influence operations (248). Detailed knowledge of a psychological profile enables manipulation techniques that expose hidden vulnerabilities rooted in childhood digital exposure. By examining sharenting data, adversaries can identify specific weaknesses, such as family dynamics, health issues, or psychological traumas (Stephenson et al. 2024). Such information facilitates the development of personalized social engineering tactics, representing a threat to democratic processes and national cohesion. Foreign services build dossiers tracking an individual's emotions and relationships from birth, utilizing emotional triggers for the recruitment or blackmail of future sensitive-position holders before they even enter office.

Beyond immediate manipulation, digital footprints enable a form of "persistent surveillance" that can last for decades. With advancements in predictive analytics, initial parental posts evolve into tools for social sorting and the monitoring of future generations

(Stephenson et al. 2024). The ecosystem of dataveillance firms creates profiles distributed to recruitment agencies and educational institutions, using algorithms to predict future behavior and loyalty (Haley 2020, 1010). Concerns are also rising about state surveillance that integrates data from social networks, smart devices, and medical records, often supported by laws requiring local data storage to facilitate access by security services (Feldstein 2020, 2). The comprehensive digital cataloging of national human resources enables adversaries to "cultivate" individuals years before they become strategically relevant, thereby compromising the entire institutional system and human interaction as a constant point of potential exploitation.

GEOPOLITICAL LEVERAGE AND INFORMATION WARFARE

Sensitive personal data, including precise geolocation information (e.g., from military installations) or intimate details, may be weaponized by foreign adversaries to coerce or blackmail individuals with access to classified national information (Sherman 2024). Sharenting inadvertently reveals extensive details about family relationships, daily routines, and children's personal vulnerabilities, thereby transforming family members into potential intelligence-gathering targets. The abundance of data on children's preferences, behavioral patterns, and emotional states enables foreign actors to build psychological profiles, which serve as a critical foundation for launching sophisticated influence operations (Stegen 2025, 248). This information is utilized to construct highly credible phishing attempts[1] and other digital deception tactics targeting parents in government, military, or critical infrastructure positions.

The extensive disclosure of family details creates an optimal environment for human intelligence (*HUMINT*) operations. Such data facilitates the identification of individuals with family vulnerabilities (such as health issues or the disclosure of personal secrets) that can

[1] Phishing is a form of online scam where attackers pose as a trustworthy entity or individual, such as a bank, social media platform, or service provider, to trick people into revealing sensitive information like passwords and credit card details, or to install malicious software (Microsoft 2026).

be exploited for blackmail, recruitment, or unauthorized access to sensitive state information. The risk of "insider threats" escalates when military personnel, state officials, and intelligence operatives are targeted, as their private lives become vulnerable points of pressure for foreign adversaries. Informal online sharing of family content directly undermines state security by compromising the integrity and loyalty of key personnel, ultimately weakening national defense and intelligence capacities.

Psychological data harvested through sharenting serves as a foundation for developing effective propaganda and disinformation campaigns (Stegen 2025, 252). This phenomenon aligns with the synthetic propaganda phase, characterized by the use of artificial intelligence to construct compelling yet fraudulent content (Kazić 2025, 108). In a broader security context, such activities become an integral part of hybrid warfare, where the synergy of kinetic and non-kinetic methods aims to destabilize the cultural and value-based foundations of the targeted state (Đorđević and Miljković 2025, 169). By understanding the psychological biases and fears within a population, foreign opponents can shape narratives that erode public trust in institutions. The psychological and social damage identified as a consequence of sharenting (e.g., the erosion of family trust, mental health issues, and the generational privacy gap) can be further weaponized in foreign influence operations (Stephenson et al. 2024).

The psychological information, social patterns, and internal conflicts of a population (including its youth) contained in sharenting data provide foreign adversaries with sophisticated tools to execute successful information warfare operations. This can involve micro-targeting propaganda to specific demographics, amplifying existing societal divisions (e.g., intergenerational conflicts over privacy, parental rights vs. child rights), or systematically eroding public trust in government, media, and democratic processes. For a country like Serbia, which is undergoing democratic reforms and pursuing EU accession, such external manipulation, fueled by readily available personal data, poses a significant threat to its democratic stability, social cohesion, and national security (Eurochild 2025). Foreign actors can use this method to quietly shape public attitudes and intensify social conflicts while damaging trust in national institutions

without conducting direct cyberattacks on infrastructure. The gradual breakdown of social unity, combined with weakened democratic institutions and increased susceptibility to foreign influence, creates a major indirect threat to national security. In a geopolitically sensitive region like the Balkans, where historical tensions can be easily reignited, this data-driven information warfare poses a particularly acute risk to Serbia's future stability and security.

CONTEXTUAL VULNERABILITIES AND DATA GOVERNANCE CHALLENGES IN THE REPUBLIC OF SERBIA

While these risks are global in scope, they take on a specific urgency within the Republic of Serbia. Here, a unique intersection of high digital engagement among youth and a lack of "digital hygiene" among parents creates a fertile ground for exploitation. As citizens navigate these external threats, the domestic legal and security infrastructure continues to wrestle with significant protective gaps.

The Constitution of the Republic of Serbia provides for the protection of privacy (Art. 41) and personal data (Art. 42) (Ustav Republike Srbije, Art. 41 i 42, 2006). These provisions constitute data collection boundaries that protect personal information from misuse, except when necessary for criminal investigations or national security. Since 2019, Serbia has implemented the Personal Data Protection Act (PDPA), which is largely aligned with the EU General Data Protection Regulation (GDPR) (Đerić, Radović, and Petrović 2025). The Personal Data Protection Act requires users to obtain consent before processing data, but imposes additional consent requirements and grants data subjects the right to request the complete removal of their data ("right to be forgotten"). For minors under 14, parental or guardian consent is generally required for data processing (Letslaw 2024).

The Commissioner for Information of Public Importance and Protection of Personal Data – DPA is the primary regulator for data protection in Serbia, with investigative, corrective, and advisory powers similar to those of GDPR supervisory bodies. However, while the DPA conducts inspections (731 in 2023) and issues warnings (51 in 2023), the number of initiated misdemeanour proceedings (ten in 2023)

appears limited given the scale of potential violations. The DPA also faces legal challenges, including lawsuits from the Ministry of Internal Affairs regarding data deletion orders (Đerić, Radović, and Petrović 2025).

Despite international human rights instruments like the UN Convention on the Rights of the Child (Art. 16 and 19) that protect children's right to privacy, Convention for the Protection of Individuals about Automatic Processing of Personal Data which ensures respect for human rights in personal data processing (Zakon o potvrđivanju konvencije o zaštiti lica u odnosu na automatsku obradu ličnih podataka [ZPKZL] 2010), Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) that criminalizes online child pornography and "grooming",[2] Serbia currently lacks a comprehensive Law on Child Rights. Instead, child-related legal provisions are part of various national laws (education, health, social welfare, etc.). Besides that, the main oversight body, the Council for the Rights of a Child, remains inactive despite its re-establishment in March 2023 (Eurochild 2023).

The current legal system provides extensive general data protection but fails to establish specific, robust standards to protect children's digital privacy in situations involving parental data sharing. Also, the enforcement mechanism lacks sufficient scale to handle the widespread nature of sharenting practices. This creates a permissive environment for sharenting, creating a huge amount of opportunities for foreign adversaries to exploit the collected sensitive child data.

The Republic of Serbia possesses an evolving cybersecurity ecosystem that faces challenges arising from both external threats and systemic complexities in data governance. Official national data reveals a structural vulnerability: a dramatic surge in mobile data consumption and digital connectivity, with mobile internet traffic continuing to grow exponentially (RATEL 2024, 22). While Serbian legislation provides a framework for combating cybercrime, the

[2] Grooming is the term used for the process that typically precedes the sexual abuse of children, often translated as "recruitment" or "luring". It involves a potential predator befriending a child and gaining their trust in an attempt to involve them in abusive sexual activities (Nacionalni kontakt centar za bezbednost dece na internetu 2023).

effectiveness of its implementation remains a subject of academic debate. Concerns have been raised about the operational capacity of the National Computer Emergency Response Team (*CERT*) to manage the scale of data exploitation facilitated by sharenting (Dennis 2024). This gap between legislative intent and operational reality creates a strategic opening for foreign actors to harvest psychological data and conduct sophisticated influence operations (Stegen 2025, 248). The discourse on digital privacy in Serbia is significantly shaped by the presence of advanced forensic and surveillance technologies. Scholarly analyses and civil society reports have raised questions regarding the oversight mechanisms governing the use of tools such as sophisticated spyware and mobile forensics (Ristić 2023, 17–19; Amnesty 2024). From a national security perspective, the central issue is not merely the existence of these capabilities, but the "trust deficit" they may generate within the population. A lack of transparency in data processing by state institutions can erode public confidence, leading to lower compliance with essential "digital hygiene" and cybersecurity protocols (Ristić 2023, 15). Further complications in this field stem from documented vulnerabilities in large-scale public databases, underscoring the technical and systemic risks within the national digital infrastructure. For instance, the centralisation of sensitive citizen data in facilities like the State Data Centre, while aimed at protection, simultaneously creates a significant target for potential exploitation and unauthorised access (10). In this context, the erosion of public trust becomes a strategic vulnerability. A population skeptical of domestic data governance is more susceptible to external influence and to sophisticated data exploitation by foreign adversaries. Therefore, the resilience of Serbia's national security is inextricably linked to the transparency of its digital oversight and the robustness of its data protection mechanisms.

Through multiple domestic and international initiatives, Serbia demonstrates its dedication to protecting children online and enhancing public awareness of digital risks. The National Contact Centre for Child Safety on the Internet has served as the key national initiative since 2017, delivering advisory support, referring abuse cases to relevant institutions, and conducting preventive educational activities at the school and community levels (European Union 2025).

Organization UNICEF Serbia also actively works with government entities and private sector companies to build protected digital spaces for children (UNICEF Serbia 2017). These initiatives include extensive educational programs that build children's digital literacy skills alongside their parents and teachers through the use of "Smart and Safe" platforms. For example, in 2023, the National Contact Centre performed 120 educational sessions throughout Serbia 2023 which brought benefits to 7,800 students, 1,000 parents, and 300 teachers (European Union 2025). Serbia also participates in global programs aimed at protecting users' online privacy. It is a party to the Council of Europe's Convention on Cybercrime (Budapest Convention) and the Lanzarote Convention, which address cybercrime and child sexual exploitation. Furthermore, Serbia collaborates with Interpol on projects like "Disrupting Harm", aimed at combating online child sexual exploitation and abuse through evidence-based research and response strategies (OSINT 2025). Despite these commendable efforts, persistent gaps remain. Public awareness of cybersecurity in Serbia is improving, but needs further improvement (Dennis 2024). Many parents still lack sufficient knowledge regarding online threats and rarely use technical parental controls. Research indicates that children often help parents with digital tasks, thus revealing a knowledge deficit among adults that current educational initiatives may not effectively resolve (Kuzmanović et al. 2019).

While Serbia's sharenting prevention initiatives demonstrate strong intent and broad reach, ongoing parent education challenges and weak implementation of technical safeguards indicate these programs have not achieved sufficient scale to change widespread sharenting behaviors and minimize associated data exposure risks. The program's focus on internet safety might not fully tackle the complex methods that sophisticated actors use to gather and weaponize data. This indicates that the current approach shows positive signs but appears inadequate to address both widespread sharenting practices and sophisticated foreign-adversary data-exploitation methods. It is a race against time where the data collection is outpacing public awareness. This means that a significant portion of Serbian society remains exposed to the indirect national security risks of sharenting, as their data flows into open-source platforms where it becomes vulnerable to exploitation.

STRATEGIC RECOMMENDATIONS FOR ENHANCING NATIONAL SECURITY RESILIENCE

To adequately address the indirect implications of sharenting for the Republic of Serbia's national security, a comprehensive, coordinated strategic approach is essential. These strategic recommendations focus on reinforcing legal frameworks, upgrading cyber protection, promoting digital literacy, and fostering international cooperation.

The enactment of a dedicated Law on the Rights of the Child should be a primary priority for Serbia in the domain of child rights protection. It is necessary for this new legislative act to address digital privacy, sharenting, and child consent through unified, comprehensive legal provisions rather than fragmented solutions. The law should include clear regulations regarding the "right to be forgotten", which children could exercise upon reaching maturity, enabling them to request the deletion of content posted by parents or third parties. Furthermore, the Commissioner for Information of Public Importance and Personal Data Protection – DPA must receive increased funding, advanced technical tools, and specific authority to conduct investigations and sanction violations related to sharenting and the exploitation of children's data (Đerić, Radović, and Petrović 2025). This body must precisely define its jurisdiction regarding parental data sharing and ensure effective processing of all received complaints.

The legal system requires continuous education programs focused on digital privacy, sharenting, and data aggregation and exploitation within the context of children's rights and national security, specifically designed for members of the police, judges, and prosecutors (Gatto, Corsello, and Ferrara 2024). This will facilitate a more subtle and effective legal response to modern digital threats. Additionally, the Government of Serbia must intensify efforts to align data protection and digital service standards with European Union frameworks, particularly the Digital Services Act (DSA). Through this measure, Serbia would achieve better oversight of online platforms operating within its territory, as well as more effective mechanisms for suppressing harmful content and data misuse.

Alongside legal reforms, it is essential to secure critical technical infrastructure. National security authorities should implement rigorous cybersecurity measures to protect vital state databases and essential services as part of a critical infrastructure defense initiative. Protecting these systems is fundamental, as hackers could cross-reference stolen data with information gathered through sharenting to create complex individual profiles (Dennis 2024). The application of "data protection by design" and "data protection by default" principles must become mandatory for every digital service and state system. This involves encouraging data minimization (collecting only necessary information) while utilizing strong encryption and other security measures. Furthermore, operational plans must be developed to prevent data brokers from selling information about Serbian citizens to foreign adversaries. These brokers should be regulated through legislation or intelligence operations to block such data transfers (Sherman 2024). The state must establish strict procedures to protect public databases containing citizen information from unauthorized access. Any data leak from state registries that coincides with sharenting information enables the creation of detailed profiles that hostile entities can easily exploit.

Long-term societal immunity depends on a systemic shift in digital literacy and education. It is imperative to launch advanced public awareness campaigns that explicitly demonstrate how sharenting compromises national security. By utilizing a narrative-driven approach, educational frameworks should illustrate how routine content sharing facilitates the "weaponization of data", transforming private family moments into permanent security vulnerabilities. Emphasis should be placed on the nation's collective security and the long-term consequences for children's futures. Additionally, mandatory digital literacy should be introduced into the educational system, from early childhood through adolescence. The curriculum should train students in critical thinking regarding online content, privacy management, and understanding the permanent digital footprint.

In parallel with systemic measures, it is essential to empower parents with practical, culturally tailored resources that enable the immediate application of privacy protection strategies, such as face-blurring techniques or rigorous control over metadata and

PII. In this context, public figures and influencers in Serbia bear a specific social responsibility to lead by example in promoting ethical sharenting and digital discretion (European Union 2025). At the macro level, Serbia's national security must be bolstered through intensive cross-border cooperation. This entails strengthening partnerships with institutions such as the European Union, UNICEF, Interpol, and Europol, primarily through the exchange of operational intelligence regarding sophisticated forms of digital child exploitation. For these efforts to materialize, sustained support for the capacity building of domestic law enforcement and intelligence agencies is mandatory, with a particular focus on advancing digital forensics and expertise in OSINT and SOCMINT analytics (Conti et al. 2024). Finally, the Government of Serbia should position itself on the international stage as a champion of global standards for protecting children's digital rights. Such strategic action aims not only to protect individuals but also to systemically curb the unchecked exploitation of data by commercial and state actors, thereby essentially safeguarding information sovereignty and the nation's future in the information age.

CONCLUSION

Sharenting today transcends the boundaries of private family practice and has become a key factor within the national security domain of the Republic of Serbia. The inadvertent creation of permanent digital identities for children, coupled with the systemic aggregation of sensitive data by commercial entities, transforms personal information into strategic intelligence resources. External actors can exploit these sources for psychological profiling, long-term surveillance, and influence operations, thereby potentially compromising the integrity of key personnel and eroding social cohesion.

The specific nature of the digital environment in Serbia is reflected in the disproportion between high internet engagement among the youth and a deficit in digital literacy among parents. Although the domestic legal framework is largely aligned with international standards, mitigating the negative effects of sharenting is hindered

by the absence of specific legislation on children's rights and by challenges in implementing existing regulations. In this context, transparency in state surveillance mechanisms is crucial for building public trust. A deficit in this trust is not merely an internal social issue, but a systemic vulnerability that weakens national resilience, rendering the population more susceptible to sophisticated external pressures and data manipulation.

Addressing this phenomenon is not exclusively a matter of individual privacy protection but constitutes a national security imperative. Building resilience requires a proactive approach that integrates strengthening legal mechanisms, improving state data governance, and large-scale digital education. Protecting the digital future of the youngest citizens is a fundamental prerequisite for preserving the long-term stability and integrity of the Republic of Serbia within a global, data-driven order.

REFERENCES

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 won't." *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. "Parent' 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/en/page/izvestaji-o-trzistu.

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.

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

Резиме

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 нарушити друштвену кохезију. Постојеће рањивости националног сајбер-безбедносног система, праћене изазовима у имплементацији легислативе, стварају амбијент погодан за експлоатацију података.

* Имејл адреса: bogdana.stjepanovic@ips.ac.rs; ORCID: 0000-0002-9504-473X.

** Имејл адреса: srdjanadjurasevic98@gmail.com; ORCID: 0009-0009-0141-7442.

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.

* This paper was received on August 6, 2025, and accepted for publication at the Editorial Board meeting on February 27, 2026.

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.