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.