UDC 342.721(497.11)
DOI: 10.5937/spm96-64569
Review article

Српска политичка мисао
(Serbian Political Thought)
No 2/2026.
Vol. 96
pp. 77-90

Goran D. Matić*

Faculty of Business Studies and Law,
Union – Nikola Tesla University, Belgrade
Military Academy, University of Defence, Belgrade

SYSTEMIC AND CULTURAL PROTECTION OF PRIVACY IN SERBIA: TOWARDS A COMPREHENSIVE LAW IN A TRANSITIONAL CONTEXT

Abstract

This paper examines the normative, institutional, and cultural framework for privacy protection in the Republic of Serbia, focusing on the challenges of artificial intelligence and digital transformation. The core assumption is that current regulation fails to provide comprehensive and sustainable protection of privacy as a fundamental right. The methodology relies on normative, comparative, and critical analysis of constitutional provisions, legislation, institutional reports, and practice. Results reveal legal fragmentation, weak implementation, and limited public and institutional awareness. The conclusion emphasises the need for constitutional reform, the adoption of a systemic privacy law, and the development of cultural infrastructure to protect digital dignity.

Keywords: privacy, human rights, digital dignity, cultural awareness, transitional context

* E-mail: goran.matic@nsa.gov.rs; ORCID: 0000-0001-8443-5797

INTRODUCTORY CONSIDERATIONS

The concept of privacy is rooted in profound legal and cultural traditions. In American legal theory, privacy was initially defined as "the right to be left alone" (Warren and Brandeis 1890), laying the foundation for its institutional protection. In contrast, Eastern European and Balkan states, including Serbia, developed within authoritarian systems in which privacy was frequently subordinated to broader ideological imperatives. In continental legal systems, privacy evolved through the doctrine of spheres – intimate, personal, and public – where the protection of dignity and autonomy over one's individual life formed its conceptual core. The security of personal data constitutes only one aspect of this broader framework, which also encompasses physical, communicational, and psychological autonomy (Westin 1967).

During the post-socialist transition, the approach to human rights in Serbia gradually shifted, yet privacy did not attain a stable normative status or sufficient social embeddedness. It remains a peripheral theme in public discourse and collective perception, underscoring the need to reevaluate cultural patterns – particularly in the context of democratic consolidation.

The contemporary digital environment introduces new challenges. Privacy is no longer confined to the protection of personal data but also includes spatial autonomy, confidentiality of communication, psychological security, and protection against algorithmic surveillance, shaming, and reputational harm (Solove 2007, 126–129; Zuboff 2019, 212–215). In Serbia, the legacy of socialist governance, the political instrumentalisation of the media, and the dominance of tabloid culture contribute to perceptions of privacy as an obstacle to public interest rather than a fundamental human right.

The Constitution of the Republic of Serbia contains several provisions related to privacy – namely, the inviolability of the home (Art. 40), secrecy of communication (Art. 41), personal data protection (Art. 42), and human dignity (Art. 19) – but lacks a unified formulation that defines privacy as an autonomous and indivisible right (Ustav Republike Srbije 2006). This normative gap hinders judicial implementation and institutional response, particularly in contexts involving digital processing, media intrusions, and low legal predictability (Matić 2025).

The methodological framework is based on the analysis of normative materials, comparative constitutional review, institutional

evaluation, and cultural interpretation of social attitudes. The applied methods include normative analysis (*lex lata* and *lex ferenda*), sociological interpretation of legal practice, and comparative examination of constitutional and legislative structures. The research relies on both primary and secondary sources – domestic legislation, oversight body reports, relevant judgments from the European Court of Human Rights, and scholarly literature from legal, sociological, and technology ethics domains. This interdisciplinary approach enables an understanding of privacy not solely as a legal category but also as a cultural and political construct (EU AFRCE 2018).

This paper aims to provide an analytical overview of the normative, institutional, and cultural framework of privacy protection in Serbia, with particular attention to the challenges posed by digital transformation and the application of artificial intelligence. The key research question is whether Serbia should adopt a systemic Privacy Law that consolidates fragmented regulations, aligns them with Article 8 of the European Convention on Human Rights (Council of Europe 1950), and ensures sustainable protection of citizens' digital dignity.

FRAGMENTATION OF LEGAL PRIVACY PROTECTION IN SERBIA

In the digital era, the right to privacy is increasingly reduced to the regulation of personal data processing. However, it comprises a much broader domain – including autonomy over individual life, spatial and communicational integrity, psychological security, and protection against algorithmic surveillance (Matić 2024a). In the Republic of Serbia, the legal framework remains fragmented and operationally uncoordinated, lacking a comprehensive law that incorporates the essential dimensions of privacy. Although the Constitution outlines fragmented safeguards – personal integrity (Art. 25), inviolability of the home (Art. 40), secrecy of communication (Art. 41), and personal data protection (Art. 42) – these provisions function mainly as declarative guarantees, without effective judicial enforcement or integration with subordinate regulations (Ustav Republike Srbije 2006). The 2018 Law on Personal Data Protection, harmonised with the GDPR, focuses on institutional data processing, leaving other privacy violations – such as media harassment and digital intrusion – beyond its scope (Zakon o zaštiti podataka o ličnosti 2018).

The Criminal Code contains provisions on privacy infringements (Arts. 146–148), yet they are applied infrequently and inconsistently. According to the Ministry of Justice (2023), only 19 proceedings were initiated for unlawful data processing, and there were no final rulings in media-related cases. This institutional inertia contributes to legal passivity: citizens are left to rely on individual effort, without systemic support or predictability of outcome (Matić 2024b).

In the digital environment, problems are further intensified. Corporations and platforms utilise personalised models based on big data, often without substantive consent. Although formal informed consent is required, it is typically reduced to non-transparent, impractical clauses – unreadable, standardised, and lacking real choice or refusal options (Zuboff 2019, 270–274; Stojković 2021, 84).

Oversight institutions – primarily the *Commissioner for Information of Public Importance and Personal Data Protection* – operate under constrained resources and limited mandates. In 2022, of 612 privacy-related complaints, only 23% led to corrective measures (Poverenik za informacije od javnog značaja 2023, 17). Unlawful data processing, online coercion, and data manipulation remain widespread, while enforcement mechanisms are seldom activated. The *Protector of Citizens (Ombudsman)* intervenes in cases of constitutional violations committed by public authorities. In contrast, the *Commissioner for the Protection of Equality* acts only when privacy breaches serve as a means of discrimination.

In conclusion, although privacy is recognised de jure, its realisation de facto remains restricted. A transparent and systematically conceived legal framework is needed to overcome fragmentation, ease the burden of proof, and provide accessible and adequate protection in line with Article 8 of the European Convention on Human Rights (Council of Europe 1950, Art. 8).

LEGAL AMBIGUITY AND LIMITED PRIVACY PROTECTION MECHANISMS

The Constitution of the Republic of Serbia does not conceptualise privacy as an autonomous and indivisible right; instead, it addresses its individual components – dignity, personal integrity, confidentiality of communications, and data protection – in a segmented manner (Ustav Republike Srbije 2006). This fragmentation produces normative

ambiguity and undermines legal enforceability, particularly within digital and media contexts (Matić 2025). Although the Constitutional Court holds competence to assess constitutionality and adjudicate constitutional complaints, its jurisprudence in matters of privacy remains scarce and underdeveloped.

Article 8 of the European Convention on Human Rights (Council of Europe 1950) ensures comprehensive protection of private and family life. The Venice Commission, in 2007, identified a misalignment between Serbia's constitutional architecture and European standards – an inconsistency later substantiated through judgments of the European Court of Human Rights against Serbia in cases involving media exposure and unauthorised data processing (Venice Commission 2007, 5).

Although criminal, civil, and administrative mechanisms are available, their application is inconsistent. In 2022, only 27 criminal complaints were filed under Articles 146–148 of the Criminal Code, with no final convictions in cases involving the media (Ministry of Justice 2023, 8). Civil litigation for non-material damages remains theoretically accessible, but procedural complexity and prohibitive costs render it largely unattainable. Institutional dispersion and limited operational capacity further obstruct meaningful protection (Matić 2024b).

The 2018 Law on Personal Data Protection (Zakon o zaštiti podataka o ličnosti 2018), aligned with the GDPR, emphasises procedural and technical aspects of data processing but neglects broader privacy violations. Only 24% of complaints submitted to the Commissioner result in corrective measures, with the institution operating under constrained resources and capacities (Poverenik za informacije od javnog značaja 2023, 17; Stojković 2021, 82). While civil action is permitted, it is pursued infrequently – fewer than ten cases annually.

The Protector of Citizens (*Ombudsman*) acts in cases of constitutional violations committed by public authorities but lacks jurisdiction over the media and the judiciary, thereby restricting the institution's scope (Zaštitnik građana 2025). The Commissioner for the Protection of Equality intervenes only when privacy violations function as instruments of discrimination – for instance, in the dissemination of intimate data intended to humiliate marginalised groups (Poverenik za zaštitu ravnopravnosti 2025).

A further institutional deficit is the absence of a *habeas data* mechanism, which would grant individuals active control over their personal sphere, including access, correction, and restriction of data

processing (Matić 2024a). Widely adopted in France, Germany, Spain, and Argentina, this legal instrument provides enhanced privacy safeguards vis-à-vis institutions and technological platforms. Serbia's omission of such a mechanism reflects a conceptual gap: privacy remains confined to data regulation rather than being approached as an integrated domain encompassing digital identity, communicative autonomy, and informational self-defence (Matić 2025).

Regional practices confirm that neighbouring countries likewise fall short of treating privacy as a systemic right. Slovenia's Constitution guarantees the inviolability of privacy (Ustav Republike Slovenije 1991), with the Information Commissioner holding a stable institutional mandate and developed complaint pathways (Informacijski pooblaščenec 2023). Croatia's Constitution protects personal data (Ustav Republike Hrvatske 2014), and the GDPR Implementation Act introduces a *habeas data* mechanism – yet an integrated definition of privacy remains absent (AZOP 2024). In Montenegro and North Macedonia, privacy is regulated indirectly through data legislation, amid limited institutional resources and uneven enforcement, especially in digital contexts.

Serbia shares structural vulnerabilities with Montenegro and North Macedonia: a lack of constitutional articulation of privacy, reliance on technical regulatory frameworks, insufficient judicial practice, and limited institutional capacity. While Slovenia and Croatia offer more functional models of data protection, neither state defines privacy as an indivisible, legally embedded right. This regional deficiency underscores the need for conceptual renewal within the legal systems of post-socialist societies.

In summary, Serbia faces three foundational obstacles: normative regulation absent effective implementation, institutional incoherence, and prevailing sociocultural apathy toward privacy. Without constitutional amendment, comprehensive legislation, and robust interinstitutional coordination, privacy remains a formal entitlement – substantively unreachable. Establishing a legal and cultural framework in which privacy stands as equal to freedom of expression and the right to human dignity is a prerequisite for its genuine protection in the contemporary era.

CULTURAL AND LEGAL PRACTICES OF PRIVACY IN SERBIA

Despite constitutional and statutory guarantees – such as the inviolability of the home, the secrecy of communications, and the protection of personal data – privacy in Serbia has yet to become a firmly embedded social value. A clear gap persists between normative guarantees and cultural perceptions. Citizens often overlook privacy violations as legally actionable, while institutional responses remain ad hoc and uneven (Stojković 2021, 9).

In sociocultural practice, privacy is seldom framed as a sphere of individual self-determination. Everyday behaviours such as commenting on private choices, posing intimate questions at the workplace, using personal photographs without consent, or expecting perpetual online availability tend to elicit little societal resistance.

The media further reinforces the normalisation of privacy violations. Tabloid coverage encourages the publicising of intimate details about public figures and their families, while reality programming systematically nullifies privacy as a social norm. This type of communication blurs the boundary between public and private, promoting publicising intimacy as a mode of social engagement (Čolović 2014, 117–121). The normative deficit is reflected in the symbolic value system, where privacy is denied the standing of a moral entitlement and remains relegated to a marginal legal category – especially within digital and media exposure contexts.

This cultural disembeddedness manifests in legal practice. Judicial remedies tend to be proceduralistic and delayed. Cases involving offences such as unauthorised photography or unlawful information gathering are rarely pursued, and judgments awarding non-material damages for privacy violations are exceptionally rare. Institutions often treat privacy as a subsidiary issue within broader legal domains – such as reputation, family relations, or security – suggesting that it is not recognised as a distinct legal interest (Antonić 2013, 201).

The notion of privacy was introduced into Serbian legal discourse primarily through the implementation of international instruments such as the European Convention on Human Rights and the GDPR, yet without deeper normative internalisation or cultural adaptation. In contrast to democratic societies where individuals actively manage their personal data and digital identity, in Serbia, the notion of personal digital

space remains poorly understood and insufficiently regulated (Matić 2024a).

Neither the media, institutions, nor the general public operates under the premise that every individual possesses an inviolable zone of privacy requiring protection, irrespective of public status or security concerns. Privacy remains relegated to the periphery, rather than upheld as a pillar of personal freedom, dignity, and self-governance.

PROPOSALS FOR ENHANCING THE CULTURE AND LEGAL PROTECTION OF PRIVACY IN SERBIA

As privacy in Serbia remains far from firmly entrenched as a legal and cultural norm, a multidisciplinary approach is essential – one that integrates educational reform, institutional development, and normative clarification. Privacy surpasses the technical realm of data protection; it includes human dignity, intimacy, communicative control, and the right to digital withdrawal (Stojković 2021, 9). The first step is raising public awareness. Media and educational campaigns should affirm privacy as a fundamental right in the digital age. Topics such as informed consent, digital security, and personal information management must become integral to both formal and informal education, with particular emphasis on youth and online environments.

At the institutional level, the mandates of the Commissioner for Information and the Protector of Citizens (*Ombudsman*) should be expanded, and specialised units within law enforcement and prosecutorial bodies should be established to address digital privacy violations. Systematic government–civil society collaboration should be institutionalised, especially for vulnerable groups. Normatively, Serbia must adopt either a comprehensive Privacy Act or a National Strategy that consolidates existing legislation, harmonises it with EU standards, and adapts it to the local context. Legal concepts such as "informed consent," "surveillance," and "automated decision-making" must be clearly defined. Public institutions and private entities should be legally obliged to publish transparent privacy policies – thus reinforcing legal predictability and citizen trust.

Regulation unsupported by cultural change remains hollow. The adoption of ethical codes and media self-regulation that prohibit unauthorised disclosure of private content is a prerequisite for normative transformation. Continued support for research, civil society initiatives,

and public debate on digital rights, the right to be forgotten, and the protection of personal autonomy is vital.

Privacy must be affirmed as a democratic value, on par with freedom of expression and minority rights. Without this cultural foundation and institutional support, legal protections remain isolated and superficial. Strategic education, institutional synergy, and internalised public awareness constitute the core pillars for establishing a sustainable framework for protecting digital dignity.

INFORMATIONAL PRIVACY AND AI CHALLENGES IN SERBIA

Digital transformation has redefined informational privacy, which now extends beyond institutional data processing to encompass algorithmic governance, digital identity, and rights to spatial and communicational autonomy. As a complex right, it is inherently tied to personal liberty and human dignity. However, privacy is increasingly reduced to technical regulation. At the same time, artificial intelligence (AI), as a systemic tool of mass data processing, exacerbates protection challenges – particularly in Serbia, where institutional structures remain underdeveloped (European Commission 2021, 3).

Informational privacy entails individual control over the collection, storage, use, and sharing of digital footprints. AI introduces risks such as automated profiling, behavioural analysis, emotion recognition, and automated decision-making, potentially leading to AI-driven discrimination, mass surveillance, and infringement of fundamental rights (Zuboff, 2019, 272–275).

In Serbia, these concerns have only recently entered legal and public discourse. The 2018 Personal Data Protection Law, though harmonised with the GDPR, does not explicitly regulate AI practices such as profiling or emotional analytics, leaving room for non-transparent processing with limited oversight. The Commissioner for Information lacks the technical instruments required for algorithmic transparency assessments, and interdisciplinary collaboration between legal, ethical, and technological institutions remains absent.

Low digital literacy undermines individual safeguards (Savić 2020, 81–83). Most citizens lack familiarity with digital processing mechanisms and related rights, while the concept of algorithmic governance remains abstract in public debate.

In such a landscape, AI poses threats to legal certainty and compromises human dignity. Robust regulation should situate data processing within a privacy-rights framework, mandating rights-based impact assessments, human supervisory obligations, and algorithmic transparency.

Simultaneously, ethical AI frameworks should codify standards for use in both the public and private sectors, grounded in principles of responsibility, intervention, and accessibility (Jobin, Ienca, and Vayena 2019, 390). Establishing independent bodies for algorithm audits and the suspension of high-risk systems, alongside sustained public education, will form the backbone of digital safety. Promoting literacy in legal, technological, and ethical dimensions must become a strategic priority. Societal understanding of AI's consequences will help ensure that technology remains subject to human values.

Although constitutional and legal provisions reference various aspects of the privacy framework, privacy is not recognised as a unified right. This gap impairs systematic responses to violations. As early as 2007, the Venice Commission recommended aligning Serbia's constitutional framework with Article 8 of the European Convention on Human Rights (Venice Commission 2007, 4). A constitutional overhaul and comprehensive privacy legislation must cover communicational, spatial, psychological, digital, and algorithmic dimensions. Only through such reform can Serbia cultivate an environment where individuals govern their identity, personal data, and digital presence – affirming privacy as a cornerstone of liberty, dignity, and autonomy in the 21st century.

CONCLUDING REFLECTIONS

This research confirms that privacy in Serbia constitutes a complex legal and cultural challenge requiring interdisciplinary solutions. Despite constitutional and statutory guarantees (e.g., the inviolability of the home, the confidentiality of communication, and the protection of personal data), the normative framework remains fragmented. The lack of constitutional recognition of privacy as an autonomous and indivisible right hinders its enforcement, especially in the digital sphere.

Reforms must include constitutional changes and a comprehensive privacy law regulating the physical, communicational, spatial, psychological, digital, and algorithmic aspects of privacy. Such an

approach would allow citizens to exercise control over their personal data and digital identity while ensuring alignment with European and international standards.

AI exacerbates privacy risks through mass data processing, opaque algorithms, and structural asymmetries in digital rights – calling for ethical and legal frameworks that provide transparency, accountability, and protect digital dignity (Zuboff 2019, 278–280; European Commission 2021, 5). Based on the conducted analysis, five key recommendations have been identified for building a sustainable privacy protection model:

1. Constitutional recognition of privacy as an indivisible and autonomous right, in accordance with Article 8 of the European Convention on Human Rights;
2. Adoption of a comprehensive privacy law with clearly defined protection and oversight mechanisms;
3. Promotion of cultural transformation through educational policy, media accountability, and civil society engagement;
4. Regulation of AI applications, ensuring algorithmic transparency and the preservation of human oversight;
5. Strengthening institutional coordination and intersectoral cooperation among relevant actors.

For privacy to evolve from rhetoric to reality, Serbia must implement these foundations. Without adequate legislation, education, and infrastructure, privacy will remain insufficiently protected – while its neglect continues to erode the pillars of freedom, dignity, and democratic order.

REFERENCES

Antonić, Slobodan. 2013. "Social mobility in socialist Serbia: a revisionist approach." *Sociološki pregled* XLVII (2): 145–170.

Agencija za zaštitu osobnih podataka [AZOP]. 2024. *Godišnje izvješće o radu Agencije za zaštitu osobnih podataka za razdoblje od 01. siječnja do 31. prosinca 2023. godine*. Zagreb: Agencija za zaštitu osobnih podataka.

Council of Europe. 1950. *European Convention on Human Rights*. Strasbourg: Council of Europe.

Čolović, I. 2014. *Tabloid culture and the public sphere*. Belgrade: XX vek.

European Commission. 2021. *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*. Brussels: European Commission.

European Union Agency for Fundamental Rights and Council of Europe [EU AFRCE]. 2018. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.

Informacijski pooblaščenec. 2023. *Annual report for 2022*. Ljubljana: Information Commissioner of the Republic of Slovenia.

Jobin, Anna, Marcello Ienca, and Effy Vayena. 2019. "The global landscape of AI ethics guidelines." *Nature Machine Intelligence* 1 (9): 389–399. DOI: 10.1038/s42256-019-0088-2

Matić, Goran. 2024a. *Osnove obrade i zaštite podataka*. Beograd: Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka.

Matić, Goran. 2024b. „Veleizdaja u Krivičnom zakoniku Republike Srbije." *Politika nacionalne bezbednosti* 26 (1): 145–164. DOI: 10.5937/pnb26-50033

Matić, Goran. 2025. „Kultura tajnosti u digitalnom dobu: između nužnosti, zloupotrebe i sajber bezbednosti." *Nacionalni interes* 52 (3): 147–172. DOI: 10.5937/nint52-59342

Ministry of Justice. 2023. *Statistical report on the application of criminal legislation in the field of privacy rights*. Belgrade: Ministry of Justice.

Poverenik za informacije od javnog značaja. 2023. *Izveštaj o radu Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti za 2022. godinu*. Beograd: Poverenik za informacije od javnog značaja.

Poverenik za zaštitu ravnopravnosti. 2025. *Redovan godišnji izveštaj Poverenika za zaštitu ravnopravnosti za 2024. godinu*. Beograd: Poverenik za zaštitu ravnopravnosti.

Savić, Miloš. 2020. "Digital literacy and privacy protection: status and challenges in Serbia." *Science and Society* 27 (1): 78–95.

Solove, Daniel J. 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven: Yale University Press.

Stojković, V. 2021. *Institucionalna zaštita prava na privatnost u Srbiji: analiza kapaciteta i izazova - Izveštaj br. 12.* Beograd: Beogradski bezbednosni forum.

Ustav Republike Hrvatske, „Narodne novine", br. 56/90, 135/97, 113/00, 28/01, 76/10, i – odluka Ustavnog suda broj: SuP-O-1/2014 .

Ustav Republike Slovenije, Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a, 92/21 – UZ62a in 98/25 – UZ74a

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

Venice Commission. 2007. *Opinion on the Constitution of Serbia (CDL-AD(2007)004)*. Strasbourg: Council of Europe.

Warren, Samuel D., and Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* IV (5): 193–220.

Westin, Alan F. 1967. *Privacy And Freedom*. New York: Atheneum.

Zakon o zaštiti podataka o ličnosti, „Službeni glasnik RS", broj 87 od 13. novembra 2018.

Zaštitnik građana. 2025. *Redovan godišnji izveštaj Zaštitnika građana za 2024. godinu*. Beograd: Zaštitnik građana Republike Srbije.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

Горан Д. Матић*

Факултет за пословне студије и право,
Универзитет Унион – Никола Тесла, Београд
Војна академија, Универзитет одбране, Београд

СИСТЕМСКА И КУЛТУРНА ЗАШТИТА ПРИВАТНОСТИ У СРБИЈИ: КА СВЕОБХВАТНОМ ЗАКОНУ У ТРАНЗИЦИОНОМ КОНТЕКСТУ

Резиме

Овај рад испитује нормативни, институционални и културни оквир за заштиту приватности у Републици Србији, фокусирајући се на изазове вештачке интелигенције и дигиталне трансформације. Основна претпоставка је да тренутна регулатива не пружа свеобухватну и одрживу заштиту приватности као основног права. Методологија се ослања на нормативну, упоредну и критичку анализу уставних одредби, законодавства, институционалних извештаја и праксе. Резултати откривају правну фрагментацију, слабу примену и ограничену јавну и институционалну свест. Закључак наглашава потребу за уставном реформом, усвајањем системског закона о приватности и развојем културне инфраструктуре ради заштите дигиталног достојанства.

Кључне речи: приватност, људска права, дигитално достојанство, културна свест, транзициони контекст

* И-мејл: goran.matic@nsa.gov.rs; ORCID: 0000-0001-8443-5797

** This manuscript was submitted on February 2, 2026, and accepted by the Editorial Board for publishing on April 1, 2026.