Polish Journal of Political Science

Volume 12 Issue 2 (2026)

V.12

Polish Journal of Political Science
Volume 12 Issue 2

V.12

The journal is published by the Interdisciplinary Research Center
of the University of Warsaw "Identity – Dialogue – Security"
(Interdyscyplinarne Centrum Badawcze Uniwersytetu Warszawskiego
„Tożsamość – Dialog – Bezpieczeństwo")

Editorial address
Polish Journal of Political Science

Interdisciplinary Research Center of the University of Warsaw
"Identity – Dialogue – Security"
Prosta 69, 00-838 Warsaw
email: centrum.tozsamosc@uw.edu.pl

Warsaw 2026

eISSN 2391-3991
Original version: e-book
Submit your paper: pjps@uw.edu.pl

Polish Journal of Political Science is included in:

PBN Polska Bibliografia Naukowa
Biblioteka Nauki
ERIHPLUS European Reference Index for the Humanities and Social Sciences
Central and Eastern European Online Library
BAZEKON

Volume 12 Issue 2 (2026)

Table of Contents

Articles

Book review

Polish Journal of Political Science

Krzysztof Śliwiński*

* Hong Kong Baptist University, e-mail: chris@hkbu.edu.hk, https://orcid.org/0000-0001-7316-3714

Volume 12 Issue 2 (2026)

From Securitization to Securitism. Analyzing the Evolution of the Securitization Theorem. Part III

DOI: 10.58183/pjps.01022026

Abstract

This paper is the third part of an exploration of the contemporary securitization phenomenon, which introduces "securitism," a novel concept describing a permanent state of managed insecurity that extends beyond traditional securitization frameworks. Building on foundational theories and critical analyses, it explores securitism as both an ideology and a lived condition in liberal democracies facing illiberal shifts. The study integrates diverse case studies, including counterterrorism, climate change, COVID-19, and immigration, to illustrate securitism's features: privatization of security, expertization, bureaucratization, technocratization, public-private partnerships, and AI-driven surveillance. The analysis critically examines how transnational corporations, especially tech giants, and AI technologies contribute to systemic limitations on fundamental human rights such as privacy, freedom of expression, and due process. The paper highlights accountability gaps arising from the delegation of security functions to private actors and the rise of surveillance capitalism, emphasizing the erosion of democratic oversight. Concluding, it calls for renewed democratic control and robust regulatory frameworks to

V.12

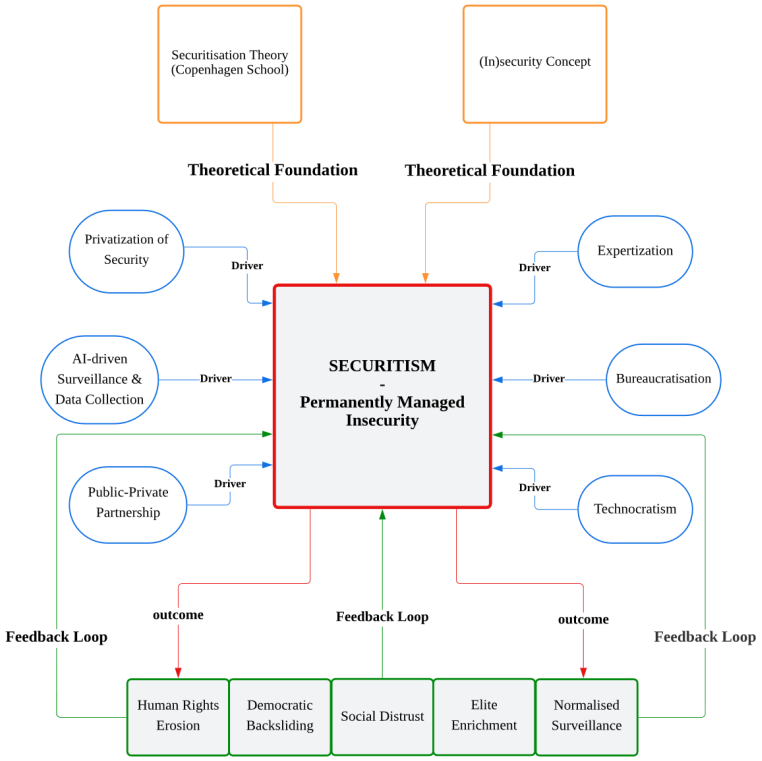
counter securitism's threats to human rights and liberal democratic governance in the 21st century.

Keywords
securitism, transnational corporations (TNCs), surveillance capitalism, artificial intelligence (AI), individual freedoms

Introduction

This article is the third part of a study devoted to the concept of securitization and its contemporary manifestations. Referring to the earlier analysis,[1] the text develops the theoretical model presented there, focusing on the mechanisms driving the consolidation of this phenomenon. In particular, this part explores two drivers of securitism: public-private partnership and data collection and the role of artificial intelligence. The paper ends with a discussion regarding the limitations of human rights.

Figure 1. Securitism Model



Source: own study.

1. K. Śliwiński, *From Securitization to Securitism. Analyzing the Evolution of the Securitization Theorem. Part II*, "Polish Journal of Political Science", 2026, Vol. 12, Issue 1, pp. 4–21, DOI: 10.58183/pjps.01012026; K. Śliwiński, *From Securitization to Securitism. Analyzing the Evolution of the Securitization Theorem. Part I*, "Polish Journal of Political Science", 2025, Vol. 11, Issue 3 (Thematic Issue), pp. 4–16, DOI: 10.58183/pjps.0103TI2025.

Volume 12 Issue 2 (2026)

Volume 12 Issue 2 (2026)

Public--Private Partnership – Unelected, Self-Serving Moguls

Big (pharma, finance, media, food, tech, or military-industrial complex) companies are the most prominent non-state actors driving and benefiting from securitism.

The literature on public-private partnerships and the role of transnational companies (TNCs) regarding existing and potential limitations of individual freedoms appears to be unequivocally negative. TNCs have emerged as powerful global actors whose operations increasingly intersect with and constrain individual liberties across multiple domains. Recent academic research reveals systematic patterns through which corporate power structures limit civil rights, labor freedoms, environmental justice, and democratic participation.

Interestingly, the relationship between transnational corporations (TNCs) and individual liberties has emerged as a central concern in Anglo-Saxon legal and political scholarship. Leading academic institutions across the United Kingdom, the United States, Canada, and Australia have produced extensive research documenting how corporate power systematically constrains civil rights, democratic participation, and individual freedoms. This report examines the key findings from highly cited Anglo-Saxon scholarship, focusing on the mechanisms through which TNCs limit individual liberties and the theoretical frameworks used to understand these constraints.

Anglo-Saxon scholarship has extensively documented how corporations exploit legal personhood to concentrate decision-making authority and attenuate public restraints on corporate choices. Jim Leach's influential analysis in *Daedalus* demonstrates how the Citizens United decision exemplifies the "constitutionalization of private power," where corporate constitutional and political speech doctrines extend corporate political influence and undermine democratic policy-making that protects civil rights.[2] This legal framework effectively transforms private corporate governance into a constitutional-style system that operates beyond traditional democratic accountability mechanisms.

The theoretical foundation for understanding corporate personhood's impact on individual liberties has been extensively developed in Canadian legal scholarship. Research published through leading academic networks reveals competing accountability frameworks, contractarian versus communitarian approaches, that illuminate how legal corporate form shapes accountability gaps and limits democratic control over corporate decisions that affect individual rights.[3] These frameworks

2. J. Leach, *Citizens United: Robbing America of Its Democratic Idealism*, "Daedalus", 2013, Vol. 142, Issue 2, pp. 95–101, DOI: 10.1162/DAED_a_00206.

3. P. Simons, *Developments in Canada on Business and Human Rights: One Step Forward Two Steps Back*, "Leiden Journal of International Law", 2023, Vol. 36, No. 2, pp. 363–388, DOI: 10.1017/S0922156522000784.

demonstrate that corporate legal structures systematically insulate corporate decision-making from public oversight while expanding corporate capacity to influence public policy.

Research has documented how TNCs use supply chain outsourcing and contractual shielding mechanisms to limit labor rights and civil liberties. The Rana Plaza collapse[4] serves as a paradigmatic case study, demonstrating how subcontracting enables lead firms to dissociate themselves from working condition harms while creating structural barriers to legal remedies for affected workers.[5] This mechanism represents a systematic approach to externalizing responsibility for rights violations while maintaining economic benefits from exploitative practices. Consequently, neoliberal governance frameworks enable corporations to assume social-policy roles through corporate social responsibility (CSR) and voluntary standards, effectively displacing stronger public regulation.[6] These soft-law governance mechanisms create accountability gaps for harms abroad while legitimizing corporate authority over traditionally public functions, thereby limiting the scope for enforceable civil-rights protections.

Environmental justice scholarship has provided detailed case studies demonstrating how corporate industrial policies shape civic and labor rights for marginalized communities. For example, historical analyses published in leading American academic journals document how corporate decisions about plant location, pollution, and employer-led regional policy systematically constrain employment opportunities, health outcomes, and civic participation rights for affected populations.[7]

The Bhopal disaster[8] continues to serve as an archetypal example illustrating how corporate operations can produce catastrophic rights violations while procedural obstacles prevent effective redress.[9] This case demonstrates the systematic nature of corporate structures that insulate firms from accountability while maximizing their capacity to externalize costs onto vulnerable populations.

Recent scholarship has also developed critical perspectives on "digital constitutionalism," arguing that platform governance and corporate production logics shape informational privacy and expressive space in ways that traditional legal frameworks struggle to remedy.[10] This analysis reveals how technology corporations exercise quasi-governmental authority over information flows and communication platforms, effectively creating private regulatory regimes that constrain individual expressive liberties without traditional constitutional protections.

4, The Rana Plaza collapse was one of the deadliest industrial disasters in modern history, occurring on April 24, 2013, in Savar Upazila, near Dhaka, Bangladesh. At around 8:57 a.m. local time, the eight-story Rana Plaza commercial building suddenly collapsed, killing 1,134 people, mostly young women garment workers, and injuring over 2,500 others.

5. R. Chambers, *Litigating Corporate Human Rights Information*, "American Business Law Journal", 2023, Vol. 60, Issue 1, pp. 111–174, DOI: 10.1111/ablj.12220.

6. T. Bartley, *Incorporating Rights: Strategies to Advance Corporate Accountability, Erika George (New York: Oxford University Press, 2021)*, "Business and Human Rights Journal", 2022, Vol. 7, No. 3, pp. 120–122, DOI: 10.1017/bhj.2022.32.

7. D.I. Márquez, *The Catalan Centre for Business and Human Rights: Addressing Extraterritorial Corporate Human Rights Abuses at the Subnational Level*, "Business and Human Rights Journal", 2023, Vol. 8, Issue 2, pp. 277–283, DOI: 10.1017/bhj.2023.21.

8. The Bhopal disaster, often called the world's worst industrial accident, occurred on December 3, 1984, at the Union Carbide India Limited (UCIL) pesticide plant in Bhopal, Madhya Pradesh, India. A massive leak of methyl isocyanate (MIC) gas and other toxic

The critique of technocratic constitutionalism emphasizes that legal reform must reckon with the material foundations of corporate power rather than relying purely on institutional fixes.[11] This perspective highlights how corporate consolidation in digital spheres creates structural constraints on individual liberty, requiring fundamental challenges to corporate power rather than merely procedural reforms.

Recent everyday cases regarding the role of TNCs in creating regimes that effectively limit fundamental individual freedoms are emerging. Especially in Anglo-Saxon countries like the United States and the United Kingdom, or across the European Union, private corporations, particularly tech giants, reap substantial profits from systemic limitations on fundamental individual freedoms, such as privacy and freedom of expression. This dynamic, termed "surveillance capitalism" by scholar Shoshana Zuboff, transforms personal data into a commodifiable asset, enabling behavioral prediction and targeted influence while eroding autonomy.[12] By capitalizing on regulatory gaps and compliance burdens, companies convert the erosion of freedoms into economic dominance, fostering a market where human experience fuels corporate accumulation.

Central to this is privacy's gradual dismantling. In the US, fragmented state-level laws, such as California's Consumer Privacy Act, offer patchwork protections, allowing firms like Google and Meta to harvest vast datasets from users' online activities, devices, and locations without robust federal oversight. This asymmetry empowers companies to build "behavioral futures markets," selling predictions of user actions to advertisers and third parties. For instance, Google's AdWords system, launched in 2000, monetizes real-time data extraction, generating billions in revenue by tailoring ads to inferred desires, often derived from non-consensual surveillance. Such practices limit privacy as a freedom, as individuals unwittingly surrender data for "free" services, creating dependency that bolsters corporate lock-in.[13]

The UK mirrors this, with post-Brexit data laws echoing US leniency, enabling firms to exploit lax enforcement under the Data Protection Act 2018. Companies benefit from "informational inequality," monitoring users opaquely while evading reciprocal transparency, which reduces market uncertainties and enables perfect price discrimination, charging individuals based on predicted willingness to pay. In labor contexts, surveillance tools track workers' productivity, suppressing bargaining power and wages, as seen in Amazon's warehouse algorithms that dictate quotas, enhancing efficiency and profits at the expense of fair labor freedoms.[14]

chemicals exposed over 500,000 people in the surrounding densely populated area, leading to immediate chaos as residents fled in panic. The gas cloud, carried by wind, blanketed slums and neighborhoods, causing widespread asphyxiation and burns.

9. R.E. Howard-Hassmann, *Civilising Globalisation: Human Rights and the Global Economy. By David Kinley. Cambridge: Cambridge University Press, 2009. 256p. $39.99*, "Perspectives on Politics", 2010, Vol. 8, No. 4, pp. 1195–1196, DOI: 10.1017/S1537592710002410.

10. D. Fuchs, B. Lennartz, *Business Interest in Human Rights Regulation: Shaping Actors' Duties and Rights*, "Critical Review of International Social and Political Philosophy", 2024, Vol. 27, Issue 3, pp. 339–362, DOI: 10.1080/13698230.2022.2113226.

11. D. Freeman, *Sovereignty, Human Rights and the Regulation of Transnational Corporations: A Critical Spatial Analysis of Civil Society Proposals for a Binding Treaty*, "Globalizations", 2024, Vol. 21, Issue 8, pp. 1402–1420, DOI: 10.1080/14747731.2024.2353993.

12, S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs 2019.

13. Ibidem.

14. K. Lipartito, *Surveillance Capitalism: Origins, History*, Consequences,

In the EU, the General Data Protection Regulation (GDPR) of 2018 imposes stricter consent requirements, yet companies profit from these limitations through refined data practices. Compliance enhances data quality, making inferences more accurate and valuable for sales. Fines up to 4% of global turnover incentivize minimal compliance, allowing loopholes such as aggregated profiling. Meta, for example, faced €1.2 billion in GDPR penalties in 2023 but continues extracting data across borders, using EU rules to standardize global operations and extract "surveillance rents" from behavioral modification. This erodes privacy while granting firms a competitive edge, as smaller entities struggle with compliance costs.[15]

Limitations on freedom of expression further advantage corporations. In the US, Section 230 of the Communications Decency Act shields platforms from liability for user content, allowing aggressive moderation without requiring publisher status, effectively censoring dissent to appease regulators or advertisers and thereby consolidating narrative control. The UK's Online Safety Act 2023 and the EU's Digital Services Act mandate content removal for "harmful" speech, pressuring firms to over-censor; compliance avoids fines but enables selective amplification of profitable content, marginalizing competitors.[16]

Ultimately, these erosions yield asymmetric gains: corporations amass unprecedented power, with surveillance infrastructure entrenching inequalities and predictability for profit. While posing existential threats to democracy, they sustain a trillion-dollar industry, underscoring capitalism's mutation where individual freedoms subsidize private wealth.

Tellingly, much of the COVID-19-related data is still stored and processed by TNCs. Private companies have played a critical role in the storage, processing, and management of COVID-19-related data, leveraging their technological infrastructure to support public health responses worldwide. During the pandemic, governments and health organizations relied on tech giants and specialized firms to handle massive volumes of sensitive data, including patient records, contact tracing information, testing results, and mobility trends. This involvement accelerated through emergency contracts that often bypassed traditional procurement and continued into 2025 as data systems evolved for ongoing surveillance and research. While enabling rapid response, it raised concerns over privacy, data sovereignty, and long-term access by corporations.

"Histories", 2025, Vol. 5, No. 1, p. 2, DOI: 10.3390/histories5010002.

15. M. Meaker, *The Slow Death of Surveillance Capitalism Has Begun*, WIRED 2023, https://www.wired.com/story/meta-surveillance-capitalism, (access 15.10.2025).

16. S. Zuboff, *The Age of Surveillance...*, op. cit.

Data Collection and AI Algorithms

As the previous part signaled, large amounts of data are harvested, stored, processed, and used by private subcontractors, much to the detriment of open public policymaking that should characterize liberal democratic states.

The proliferation of data collection practices by transnational corporations and governments in Western Europe presents unprecedented challenges to fundamental individual freedoms. While the European Union has been trying to position itself as a global leader in privacy protection through the General Data Protection Regulation (GDPR),[17] extensive surveillance practices continue to threaten privacy, autonomy, and democratic participation across the region.[18]

Transnational technology corporations have developed sophisticated surveillance-driven business models that systematically extract and commodify human behavior. Companies like Google, Meta, and Amazon deploy vast tracking networks across websites, mobile applications, and connected devices to create comprehensive behavioral profiles of European users.[19] As mentioned earlier, this practice is referred to as "surveillance capitalism" by scholars. It transforms personal experiences into predictive products used to influence individual choices and market outcomes.[20]

The scale of corporate data collection enables unprecedented micro-targeting capabilities that extend beyond advertising to include political messaging and behavioral modification. These practices create significant power asymmetries between individuals and corporations, undermining personal autonomy and creating what researchers describe as "data colonialism," in which social life is extracted for profit without meaningful consent.[21]

A critical concern is the inadequacy of de-identification techniques. While companies claim that anonymized data poses minimal privacy risks, research demonstrates that such protections can be easily circumvented through re-identification and inferential analytics, encouraging wider data sharing under false security assumptions.[22]

Western European governments have significantly expanded their surveillance capabilities, often justified through risk-based governance frameworks that emphasize security and efficiency over individual rights. The United Kingdom exemplifies this trend with its extensive CCTV

17. The General Data Protection Regulation (GDPR) is a European Union law that protects the personal data and privacy of individuals in the EU. It was adopted in 2016 and became effective in May 2018, and it sets strict rules for how organizations collect, use, and transfer personal data, applying to companies worldwide that handle the data of EU residents. The GDPR gives individuals more control over their data and establishes penalties for non-compliance.

18. C.J. Bennett, *The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?*, "Information Polity", 2018, Vol. 23, Issue 2, pp. 239–246, DOI: 10.3233/IP-180002.

19. J. Andrew, M. Baker, *The General Data Protection Regulation in the Age of Surveillance Capitalism*, "Journal of Business Ethics", 2021, Vol. 168, pp. 565–578, DOI: 10.1007/s10551-019-04239-z.

20. N. Couldry, U.A. Mejias, *Making Data Colonialism Liveable: How Might Data's Social Order Be Regulated?*, "Internet Policy Review", 2019, Vol. 8, Issue 2, pp. 1–16, DOI: 10.14763/2019.2.1411.

21. Ibidem.

22. J. Andrew, M. Baker, *The General Data...*, op. cit., pp. 565–578.

network, over 6 million cameras nationwide, creating one of the world's most surveilled societies.[23] London alone hosts an estimated 600,000 cameras, enabling near-continuous monitoring of public spaces.

Government surveillance extends beyond visual monitoring to include automated profiling systems for law enforcement and welfare administration. These algorithmic systems can produce opaque, consequential decisions that affect fundamental social rights, with limited avenues for individual challenge or redress.[24] The normalization of such practices through administrative efficiency arguments represents a concerning shift toward routine surveillance in democratic societies.

The transnational nature of data flows creates significant enforcement gaps that expose European residents to weaker privacy protections in third countries. Despite GDPR's extraterritorial reach, practical limitations persist in protecting EU citizens when their data is processed in jurisdictions with different legal frameworks or extensive surveillance powers.[25]

The EU-US Data Privacy Framework, designed to enable commercial data transfers while protecting privacy, has faced persistent challenges. Recent reviews have identified shortcomings in protecting EU citizens from foreign intelligence access, highlighting the difficulty of reconciling different legal traditions and security priorities across jurisdictions.[26]

Pervasive data collection creates significant chilling effects on freedom of expression and association. When individuals know their communications and activities are monitored and analyzed, they may self-censor or avoid legitimate political activities, particularly affecting activists, journalists, and political dissidents.[27]

The micro-targeting capabilities enabled by extensive data collection also threaten democratic discourse by fragmenting the shared public sphere essential for democratic deliberation. When political messages are individually tailored based on psychological profiles, it becomes difficult to maintain the common factual foundation necessary for democratic debate.[28]

While GDPR represents significant progress in privacy protection, it faces substantial implementation challenges. Enforcement remains uneven across member states, with resource constraints limiting regulatory authorities' capacity to address the scale and sophistication of modern

23. M.N. Asghar, et al., *Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective*, "IEEE Access", 2019, Vol. 7, pp. 111709–111726.

24. M. Padden, *Governing Surveillance: Digitalisation, Data Protection and Democracy*, PhD thesis, University of Edinburgh 2024.

25. A. Mattoo, J.P. Meltzer, *International Data Flows and Privacy: The Conflict and its Resolution*, Working Paper 8431, World Bank Policy Research 2018.

26. B.S. Jiménez-Gómez, *Transnational Data Transfers Under GDPR*, "InDret", 2025, Vol. 3, pp. 1–35.

27. M. Padden, *The Transformation of Surveillance in the Digitalisation Discourse of the OECD: A Brief Genealogy*, "Internet Policy Review", 2023, Vol. 12, No. 3, pp. 1–39, DOI: 10.14763/2023.3.1720.

28. C.J. Bennett, *The European General...*, op. cit., pp. 239–246.

data practices. The regulation's reliance on consent mechanisms and controller obligations struggles against the opacity and complexity of contemporary surveillance systems.[29]

In sum, the extensive data collection practices of transnational corporations and governments in Western Europe pose significant threats to individual freedoms despite regulatory protections. The concentration of data analytics capabilities creates new power asymmetries that can undermine democratic governance and personal autonomy. Addressing these challenges requires strengthened enforcement mechanisms, technological innovation that prioritizes privacy, and a renewed commitment to democratic oversight of surveillance practices. The future of individual freedom in European democracies depends on developing effective responses to surveillance capitalism and expanding state monitoring capabilities.

Furthermore, these challenges are exacerbated by the integration of artificial intelligence. Academics have increasingly raised concerns about the potential of artificial intelligence to constrain individual freedoms, particularly through surveillance, automated decision-making, and inadequate regulatory frameworks.

Contemporary AI systems enable unprecedented surveillance capabilities, fundamentally altering the relationship between individuals and institutions. Scholars warn that AI-driven surveillance creates "data doubles" through continuous monitoring and algorithmic social sorting, challenging traditional privacy boundaries.[30] Facial recognition and emotion-detection technologies are particularly concerning, as they enable real-time identification and behavioral analysis in public spaces.[31] The Cambridge Analytica scandal exemplifies how psychographic profiling can manipulate democratic processes through targeted messaging, demonstrating AI's capacity to undermine autonomous decision-making.[32]

Despite the General Data Protection Regulation's progressive framework, European academics identify critical limitations in addressing AI-specific challenges. The GDPR's retrospective controls struggle with rapid algorithmic data flows, creating a "pacing problem" where legal remedies lag behind technological development.[33] Article 22's provisions on automated decision-making are criticized as vague and insufficient, leaving many AI applications outside meaningful regulatory oversight.[34] The technical opacity of machine learning systems further undermines transparency rights, as "black box" algorithms resist meaningful explanation even when legally required.[35]

29. J. Andrew, M. Baker, *The General Data...*, op. cit., pp. 565–578.

30. M. Alfi Fadhlurrahman, S. Riyanta, M. Reza Rustam, *Algorithms and Human Rights: The Impact of AI Technology on the Protection of Individual Rights*, "Formosa Journal of Multidisciplinary Research", 2024, Vol. 3, Issue 10, pp. 3777–3792.

31. A. Shams, *Data Protection and Privacy Laws and Regulations*, in: *Democracy and Democratization in the Age of AI*, eds. K. Wongmahesak, I. Wekke, C. Seftyono, N. Nurdin, IGI Global Scientific Publishing 2025, pp. 235–258, DOI: 10.4018/979-8-3693-8749-8.ch013.

32. M. Alfi Fadhlurrahman, S. Riyanta, M. Reza Rustam, *Algorithms and Human...*, op. cit.

33. Ibidem.

34. S. Mougdir, *Artificial Intelligence in a Privacy-Concerned World: Automated Decision-Making and the GDPR*, Master's thesis, Tilburg University 2020.

35. K.D.S. Nonju, B. Ihua-Maduenyi, *The Impact of Artificial Intelligence on Privacy Laws*, "International Journal of Research and Innovation in Social Science", 2024, Vol. 8, No. 9, pp. 2150–2174, DOI: 10.47772/IJRISS.2024.8090178.

Scholars emphasize that automated decision-making systems can instrumentalize individuals, reducing human dignity and constraining meaningful choice. AI systems that allocate resources or opportunities without explainable criteria risk treating people as objects rather than autonomous agents.[36] Algorithmic micro-targeting presents particular concerns for freedom of thought, as manipulative persuasion techniques can intrude into the "forum internum," the protected space of opinion formation and decision-making.[37] These technologies create differential access to services and opportunities, thereby undermining the principles of equal treatment that are fundamental to European legal traditions.

For example, one need look no further than Palantir.[38] Palantir Technologies is a private data analytics firm co-founded by Peter Thiel and Alex Karp in 2003, which has emerged as a key subcontractor in U.S. military operations, securing over $1 billion in Department of Defense contracts, including a $795 million deal in 2025 for AI integration.[39] Its platforms, Foundry and Gotham, enable governments to fuse disparate datasets, such as social media, financial records, medical claims, and biometrics, into comprehensive individual profiles, ostensibly for enhanced efficiency in warfare and security.

In military contexts, Palantir's AI excels at rapid targeting: in Ukraine and Israel, it processes sensor data to map enemy movements and identify specific militants, such as Hamas leaders in Gaza, facilitating airstrikes with minimal human oversight.[40] Domestically, under a March 2025 executive order, Palantir merges data from agencies like the Department of Homeland Security, the Internal Revenue Service, and the Department of Health and Human Services, creating "super-databases" that profile Americans' bank details, student debt, and health records for immigration enforcement.[41] Its Investigative Case Management (ICM) system, used by the U.S. Immigration and Customs Enforcement, constructs digital dossiers on suspects, alerting agents to address changes and analyzing device data for deportations.[42]

These capabilities profoundly limit fundamental freedoms. Privacy evaporates as data repurposing risks misuse, former engineer Linda Xia warned of a "significant risk" from aggregated profiles, which enable the political targeting of critics or immigrants. Due process suffers in automated decisions, fostering a surveillance state where AI "hallucinations" could erroneously flag innocents, echoing Thiel's anti-democratic views and threatening civil liberties. As Karp boasted, Palantir aims to "scare enemies and on occasion kill them," prioritizing power over rights. This trajectory imperils democratic safeguards, urging ethical restraints.[43]

36. A. Shams, *Data Protection and...*, op. cit., pp. 235–258.

37. M. Bodimani, *AI-Powered Surveillance vs. Privacy Rights: Striking the Right Balance*, "International Journal For Multidisciplinary Research", 2025, Vol. 7, Issue 2, pp. 1–19, DOI: 10.36948/ijfmr.2025.v07i02.42672.

38. See more at: *Palantir*, https://www.palantir.com/, (access 09.10.2025).

39. P. Apps, *Military AI Revolution Heightens Competition for Defence Tech Contracts: Peter Apps*, Reuters 2025, https://www.reuters.com/technology/artificial-intelligence/military-ai-revolution-heightens-competition-defence-tech-contracts-peter-apps-2025-09-05/, (access 15.10.2025).

40. Ibidem.

41. R. Reich, *Peter Thiel's Palantir Poses a Grave Threat to Americans*, The Guardian 2025, https://www.theguardian.com/commentisfree/2025/jun/30/peter-thiel-palantir-threat-to-americans, (access 15.10.2025).

42. H. Khlaaf, *Myers West S., The Rush to A.I. Threatens National Security*, The New York Times 2025, https://www.nytimes.com/2025/01/27/opinion/ai-trump-military-national-security.html, (access 15.10.2025).

43. R. Reich, *Peter Thiel's Palantir...*, op. cit.

Discussion

The International Covenant on Civil and Political Rights, legally binding, lists no fewer than twenty-one fundamental human rights and individual freedoms:

1. The right of self-determination for all peoples, allowing them to freely determine their political status and pursue economic, social, and cultural development (Article 1);

2. Equality and non-discrimination based on race, color, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status (Article 2 and Article 26);

3. The inherent right to life and protection against arbitrary deprivation of life (Article 6);

4. Freedom from torture or cruel, inhuman, or degrading treatment or punishment (Article 7);

5. Prohibition of slavery, servitude, and forced or compulsory labor, with specified exceptions (Article 8);

6. The right to liberty and security of person; protection against arbitrary arrest or detention; rights related to arrest and detention procedures; and the right to an effective remedy if rights are violated (Articles 9 and 3(a)-(c));

7. Humane treatment and respect for the dignity of persons deprived of liberty, including fair treatment of accused persons and juveniles (Article 10);

8. Freedom of movement, including liberty to choose residence and the right to leave and enter one's own country (Article 12);

9. Fair trial rights, including equality before courts, presumption of innocence, right to be informed promptly of charges, adequate time and facilities to prepare a defense, right to legal assistance, examination of witnesses, and protection against self-incrimination (Article 14);

10. Protection against retroactive criminal laws and double jeopardy (Articles 15 and 7(g));

Volume 12 Issue 2 (2026)

11. The right to recognition as a person before the law (Article 16);

12. Protection of privacy, family, home, and correspondence from arbitrary or unlawful interference (Article 17);

13. Freedom of thought, conscience, and religion, including freedom to adopt and manifest religion or belief, subject only to restrictions necessary to protect public safety, order, health, morals, or the rights and freedoms of others (Article 18);

14. Freedom of opinion and expression, including the right to seek, receive, and impart information and ideas, with restrictions only as necessary for respect of others' rights or national security, public order, health, or morals (Article 19);

15. Prohibition of propaganda for war and advocacy of national, racial, or religious hatred that incites discrimination, hostility, or violence (Article 20);

16. The right of peaceful assembly (Article 21);

17. The right to freedom of association, including forming and joining trade unions (Article 22);

18. Protection of the family as the fundamental group unit of society and rights related to marriage, including free consent and equality of spouses (Article 23);

19. Rights of the child, including non-discrimination, registration after birth, and acquisition of nationality (Article 24);

20. Political rights, including the right to participate in public affairs, vote, be elected, and access public service without discrimination (Article 25);

21. Rights of ethnic, religious, or linguistic minorities to enjoy their own culture, practice their religion, and use their language (Article 27).

"These rights are to be respected and ensured by States Parties without discrimination, and the Covenant provides mechanisms for their protection and implementation."[44]

As the reader can clearly see, most of these rights are likely to be limited, if not completely annulled, by the governments' latest initiatives, such as Digital ID, Central Bank Digital Currency (CBDC), Personal CO2 Tracker, or health certificates. All of these devices have already been introduced to the public under the pretext of convenience or public safety (security). All of them carry the potential to limit, or even annul, most of the rights mentioned above under the internationally recognized conventions and legally binding treaties.

Against this backdrop, three more initiatives ought to be mentioned in the context of securitism as proposed by this paper. Firstly, according to the latest media reports, the Canadian Government has proposed Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.[45] Critics claim that the legislation will allow the Canadian Government to isolate Canadians from communication, information, and essential online services (e.g., banking, healthcare, or emergency alerts), infringing on freedom of expression (Section 2(b) of the Charter) and equality rights. They warn that it risks abuse against political dissidents or protesters, as seen in the 2022 Freedom Convoy, where asset freezes caused irreparable harm without due process. Without compensation for losses, economic harm is exacerbated.

Secondly, the World Health Organization (WHO) unveiled an upgraded version of its Epidemic Intelligence from Open Sources (EIOS) 2.0 system on October 13, 2025. This AI-powered platform is designed to monitor publicly available online content, including social media posts, news articles, websites, and even transcribed radio broadcasts, for signals of emerging public health threats, such as disease outbreaks, rumors, or misinformation (referred to as "infodemics"). While presented as a tool for enhancing global health security and pandemic preparedness, it has sparked significant debate over its potential to enable surveillance, narrative control, and censorship of online discourse. Below, I will break down what the system is, how it works, its stated goals, and the key criticisms regarding its impact on freedoms.[46]

Last but not least, the EU Chat Control proposal, officially known as the Regulation to Prevent and Combat Child Sexual Abuse (CSA Regulation or CSAR), is another controversial legislative initiative aimed at tackling online child sexual abuse material (CSAM). Introduced by European Commis-

44. International Covenant on Civil and Political Rights, United Nations General Assembly, General Assembly resolution 2200A (XXI), entered into force March 23, 1976, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights, (access 15.10.2025).

45. As of writing of this paper (October 2025), the bill is in second reading in the House. After passing the House, it will need to go through all three readings in the Senate before receiving Royal Assent. See more: *Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, Government of Canada 2025, https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c8_2.html, (access 15.10.2025).

46. See more: *WHO upgrades its public health intelligence system to boost global health security*, World Health Organization 2025, https://www.who.int/news/item/13-10-2025-who-upgrades-its-public-health-intelligence-system-to-boost-global-health-security, (access 15.10.2025).

sioner for Home Affairs Ylva Johansson on May 11, 2022, it seeks to expand detection and reporting obligations for online platforms. Critics, including privacy advocates such as the Electronic Frontier Foundation (EFF) and European Digital Rights (EDRi), have dubbed it "Chat Control" due to its potential to scan private digital communications, including encrypted messages, on a widespread scale. As of October 27, 2025, the proposal remains stalled amid fierce opposition, with a key vote postponed and no final adoption in sight.[47]

47. See more at: *Fight Chat Control*, https://fightchatcontrol.eu/, (access 15.10.2025).

Conclusions

This paper advances the scholarly discourse on securitization by introducing the novel concept of "Securitism," a permanent state of managed insecurity that transcends traditional understandings of securitization and (in)security. Building upon the foundational works of the Copenhagen School and the critical analyses of Bigo and Tsoukala, this study bridges significant gaps in existing literature by articulating securitism as both an ideological framework and a tangible condition within contemporary Western societies, especially liberal democracies undergoing illiberal transformations.

The originality of this work lies in its comprehensive integration of multifaceted case studies, ranging from counterterrorism and military conflicts to climate change, the COVID-19 pandemic, and immigration, that collectively reveal securitism's defining features. These include the privatization of security, expertization, bureaucratization, technocratization, public-private partnerships, and the pervasive role of artificial intelligence in surveillance and data collection. This holistic approach unveils how securitism operates not merely as a reactive security measure but as a proactive, systemic ideology that legitimizes the progressive curtailment of fundamental human rights under the guise of permanent threat management.

By critically examining the implications of securitism for democratic governance, individual freedoms, and human rights, the paper highlights its transformative impact on political authority and societal norms. The increasing delegation of security functions to private actors, the ascendancy of technocratic expertise, and the deployment of AI-driven surveillance create accountability gaps and erode democratic oversight, raising urgent normative concerns.

In sum, this work's conceptual innovation and empirical breadth offer a timely and critical framework for understanding the evolving security landscape. It calls for renewed scholarly attention and policy interventions to address the challenges securitism poses to liberal democratic values

and individual autonomy in the 21st century. The author of this study argues that there is a critical need for renewed democratic oversight and robust regulatory frameworks to mitigate the pervasive threats of securitism to human rights and democratic governance.

Bibliography

Alfi Fadhlurrahman M., Riyanta S., Reza Rustam M., *Algorithms and Human Rights: The Impact of AI Technology on the Protection of Individual Rights*, "Formosa Journal of Multidisciplinary Research", 2024, Vol. 3, Issue 10, pp. 3777–3792.

Andrew J., Baker M., *The General Data Protection Regulation in the Age of Surveillance Capitalism*, "Journal of Business Ethics", 2021, Vol. 168, pp. 565–578, DOI: 10.1007/s10551-019-04239-z.

Apps P., *Military AI Revolution Heightens Competition for Defence Tech Contracts: Peter Apps*, Reuters 2025, https://www.reuters.com/technology/artificial-intelligence/military-ai-revolution-heightens-competition-defence-tech-contracts-peter-apps-2025-09-05/, (access 15.10.2025).

Asghar M.N., Kanwal N., Lee B., Fleury M., Herbst M., Qiao Y., *Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective*, "IEEE Access", 2019, Vol. 7, pp. 111709–111726.

Bartley T., *Incorporating Rights: Strategies to Advance Corporate Accountability, Erika George (New York: Oxford University Press, 2021)*, "Business and Human Rights Journal", 2022, Vol. 7, No. 3, pp. 120–122, DOI: 10.1017/bhj.2022.32.

Bennett C.J., *The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?*, "Information Polity", 2018, Vol. 23, Issue 2, pp. 239–246, DOI: 10.3233/IP-180002.

Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, Government of Canada 2025, https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c8_2.html, (access 15.10.2025).

Bodimani M., *AI-Powered Surveillance vs. Privacy Rights: Striking the Right Balance*, "International Journal For Multidisciplinary Research", 2025, Vol. 7, Issue 2, pp. 1–19, DOI: 10.36948/ijfmr.2025.v07i02.42672.

Chambers R., *Litigating Corporate Human Rights Information*, "American Business Law Journal", 2023, Vol. 60, Issue 1, pp. 111–174, DOI: 10.1111/ablj.12220.

Couldry N., Mejias U.A., *Making Data Colonialism Liveable: How Might Data's Social Order Be Regulated?*, "Internet Policy Review", 2019, Vol. 8, Issue 2, pp. 1–16, DOI: 10.14763/2019.2.1411.

Fight Chat Control, https://fightchatcontrol.eu/, (access 15.10.2025).

Freeman D., *Sovereignty, Human Rights and the Regulation of Transnational Corporations: A Critical Spatial Analysis of Civil Society Proposals for a Binding Treaty*, "Globalizations", 2024, Vol. 21, Issue 8, pp. 1402–1420, DOI: 10.1080/14747731.2024.2353993.

Fuchs D., Lennartz B., *Business Interest in Human Rights Regulation: Shaping Actors' Duties and Rights*, "Critical Review of International Social and Political Philosophy", 2024, Vol. 27, Issue 3, pp. 339–362, DOI: 10.1080/13698230.2022.2113226.

Howard-Hassmann R.E., *Civilising Globalisation: Human Rights and the Global Economy. By David Kinley. Cambridge: Cambridge University Press, 2009. 256p. $39.99*, "Perspectives on Politics", 2010, Vol. 8, No. 4, pp. 1195–1196, DOI: 10.1017/S1537592710002410.

International Covenant on Civil and Political Rights, United Nations General Assembly, General Assembly resolution 2200A (XXI), entered into force March 23, 1976, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights, (access 15.10.2025).

Jiménez-Gómez B.S., *Transnational Data Transfers Under GDPR*, "InDret", 2025, Vol. 3, pp. 1–35.

Khlaaf H., Myers West S., *The Rush to A.I. Threatens National Security*, The New York Times 2025, https://www.nytimes.com/2025/01/27/opinion/ai-trump-military-national-security.html, (access 15.10.2025).

Leach J., *Citizens United: Robbing America of Its Democratic Idealism*, "Daedalus", 2013, Vol. 142, Issue 2, pp. 95–101, DOI: 10.1162/DAED_a_00206.

Lipartito K., *Surveillance Capitalism: Origins, History, Consequences*, "Histories", 2025, Vol. 5, No. 1, pp. 1–13, DOI: 10.3390/histories5010002.

Márquez D.I., *The Catalan Centre for Business and Human Rights: Addressing Extraterritorial Corporate Human Rights Abuses at the Subnational Level*, "Business and Human Rights Journal", 2023, Vol. 8, Issue 2, pp. 277–283, DOI: 10.1017/bhj.2023.21.

Mattoo A., Meltzer J.P., *International Data Flows and Privacy: The Conflict and its Resolution*, Working Paper 8431, World Bank Policy Research 2018.

Meaker M., *The Slow Death of Surveillance Capitalism Has Begun*, WIRED 2023, https://www.wired.com/story/meta-surveillance-capitalism, (access 15.10.2025).

Mougdir S., *Artificial Intelligence in a Privacy-Concerned World: Automated Decision-Making and the GDPR*, Master's thesis, Tilburg University 2020.

Nonju K.D.S., Ihua-Maduenyi B., *The Impact of Artificial Intelligence on Privacy Laws*, "International Journal of Research and Innovation in Social Science", 2024, Vol. 8, No. 9, pp. 2150–2174, DOI: 10.47772/IJRISS.2024.8090178.

Padden M., *Governing Surveillance: Digitalisation, Data Protection and Democracy*, PhD thesis, University of Edinburgh 2024.

Padden M., *The Transformation of Surveillance in the Digitalisation Discourse of the OECD: A Brief Genealogy*, "Internet Policy Review", 2023, Vol. 12, No. 3, pp. 1–39, DOI: 10.14763/2023.3.1720.

Palantir, https://www.palantir.com/, (access 09.10.2025).

Reich R., *Peter Thiel's Palantir Poses a Grave Threat to Americans*, The Guardian 2025, https://www.theguardian.com/commentisfree/2025/jun/30/peter-thiel-palantir-threat-to-americans, (access 15.10.2025).

Shams A., *Data Protection and Privacy Laws and Regulations*, in: *Democracy and Democratization in the Age of AI*, eds. K. Wongmahesak, I. Wekke, C. Seftyono, N. Nurdin, IGI Global Scientific Publishing 2025, pp. 235–258, DOI: 10.4018/979-8-3693-8749-8.ch013.

Simons P., *Developments in Canada on Business and Human Rights: One Step Forward Two Steps Back*, "Leiden Journal of International Law", 2023, Vol. 36, No. 2, pp. 363–388, DOI: 10.1017/S0922156522000784.

Śliwiński K., *From Securitization to Securitism. Analyzing the Evolution of the Securitization Theorem. Part I*, "Polish Journal of Political Science", 2025, Vol. 11, Issue 3 (Thematic Issue), pp. 4–16, DOI: 10.58183/pjps.0103TI2025.

Śliwiński K., *From Securitization to Securitism. Analyzing the Evolution of the Securitization Theorem. Part II*, "Polish Journal of Political Science", 2026, Vol. 12, Issue 1, pp. 4–21, DOI: 10.58183/pjps.01012026.

WHO upgrades its public health intelligence system to boost global health security, World Health Organization 2025, https://www.who.int/news/item/13-10-2025-who-upgrades-its-public-health-intelligence-system-to-boost-global-health-security, (access 15.10.2025).

Zuboff S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs 2019.