



Indonesia Media Law Review, Volume 5 Issue 1 (June 2026), pp. 1-33

ISSN 2829-7628 (Print) 2829-7423 (Online)

<https://doi.org/10.15294/imrev.v5i1.44290>.

Indonesia Media Law Review is Journal for Media, Press Law and Ethics in Journalism

Published biannually by the Faculty of Law, Universitas Negeri Semarang, Indonesia and managed by Law Student Press Community and Press and Journalism Law Studies Center, Faculty of Law Universitas Negeri Semarang, INDONESIA

Available online since

Human Rights Protection in the Ecosystem of Surveillance Technology and Big Data Law Enforcement

Safrin Salam

Faculty of Law, Universitas Muhammadiyah Buton, Indonesia

Asmah

Faculty of Law, Universitas Sawerigading, Indonesia

Muhammad Ramadan Kiro

Faculty of Law, Universitas Halu Oleo Kendari, Indonesia

Sulastri Yasim

Universitas Sulawesi Barat, Indonesia

Ibrahim Kayode Muhammed

Kwara State University, Nigeria

**Corresponding author's email: safrin.salam@umbuton.ac.id*

ABSTRACT: The rapid integration of surveillance technology and big data analytics into law enforcement has transformed contemporary governance, generating both security benefits and serious human rights concerns. This article examines how existing regulatory frameworks inadequately address the dynamic risks embedded in surveillance ecosystems and proposes a lifecycle-

based governance response. Using a qualitative normative-empirical methodology, the study combines doctrinal legal analysis of international human rights law with comparative regulatory assessment and interdisciplinary technology governance theory. The findings reveal structural fragmentation, insufficient algorithmic transparency, weak proportionality assessment, and reactive oversight mechanisms that fail to capture risks across data collection, storage, analysis, sharing, and deletion. In response, the study develops a Dynamic Human Rights Risk Assessment Model that operationalizes proportionality, necessity, transparency, and accountability at each stage of the surveillance data lifecycle. The model embeds continuous monitoring, mandatory impact assessments, and independent oversight within surveillance infrastructures, shifting governance from static compliance to adaptive human rights stewardship. The research concludes that lifecycle-based regulation provides a coherent and flexible framework capable of safeguarding fundamental rights while accommodating technological innovation in complex surveillance environments.

KEYWORDS: Surveillance Technology; Big Data Governance; Human Rights Protection

I. INTRODUCTION

The rapid expansion of surveillance technology and big data analytics has fundamentally transformed contemporary law enforcement practices, reshaping investigative methods, risk profiling, and crime prevention strategies across jurisdictions. Modern policing infrastructures increasingly operate within what scholars describe as a surveillance ecosystem an interconnected architecture of digital monitoring tools, algorithmic systems, biometric databases, and data integration platforms functioning across public and private domains.¹ As digital infrastructures merge with systems of speech regulation and monitoring, the boundaries between communication networks and surveillance apparatuses have eroded.² This structural

¹ M. Kwet, "Digital colonialism: US empire and the new imperialism in the Global South," *Race & Class* 60, no. 4 (2019): 3–26, <https://doi.org/10.1177/0306396818823172>.

² E. Ricknell, "Freedom of expression and alternatives for internet governance: Prospects and pitfalls," *Media and Communication* 8, no. 4 (2020): 110–20, <https://doi.org/10.17645/mac.v8i4.3299>.

convergence means that the same technological platforms enabling democratic participation simultaneously facilitate unprecedented monitoring of citizens' activities, associations, and expressions.

The rise of surveillance capitalism further intensifies this transformation. Big data extracted from everyday digital behavior has become commodified and concentrated in the hands of powerful corporate and state actors.³ Surveillance infrastructures now operate at the architectural level of the digital ecosystem, encompassing hardware, software, and network connectivity, thereby extending influence beyond commercial interests into law enforcement and political control.⁴ Algorithmic systems increasingly mediate law enforcement decisions, from predictive analytics to automated facial recognition (AFR), raising urgent concerns about transparency and accountability.⁵ These developments reflect not merely technological innovation but a profound restructuring of power relations between states, corporations, and citizens.

State surveillance has evolved from targeted monitoring of specific suspects to mass, population-level data collection. Empirical research demonstrates how surveillance technologies are frequently deployed asymmetrically. In China, the implementation of mandatory location disclosure on social media platforms illustrates how surveillance tools can selectively target politically sensitive groups,

³ Kwet, "Digital colonialism: US empire and the new imperialism in the Global South"; A. Meireles, "Digital rights in perspective: The evolution of the debate in the Internet Governance Forum," *Politics & Policy* 52, no. 1 (2024): 12–32, <https://doi.org/10.1111/polp.12571>; K. Riemer dan S. Peter, "Algorithmic audiencing: Why we need to rethink free speech on social media," *Journal of Information Technology* 36, no. 4 (2021): 409–26, <https://doi.org/10.1177/02683962211013358>.

⁴ Kwet, "Digital colonialism: US empire and the new imperialism in the Global South."

⁵ Meireles, "Digital rights in perspective: The evolution of the debate in the Internet Governance Forum."

disproportionately monitoring dissenting voices.⁶ Such selective surveillance undermines the principle of equality before the law and reveals that surveillance technologies are rarely neutral instruments. Similarly, in democratic contexts, counter-terrorism frameworks have institutionalized forms of pre-emptive surveillance. The United Kingdom's Prevent Duty effectively transforms educational institutions into nodes of a broader security apparatus, producing what participants describe as "modern-day panopticons" and generating widespread self-censorship among Muslim students.⁷ These developments demonstrate that surveillance infrastructures operate across political systems, albeit with different justifications and intensities.

Big data analytics further extend the reach of surveillance beyond traditional monitoring. Algorithmic systems aggregate and interpret vast datasets to identify behavioral patterns, predict risks, and flag individuals for scrutiny.⁸ The phenomenon of algorithmic audience, initially developed for commercial targeting, illustrates how speech organization and audience segmentation can be repurposed for monitoring public discourse.⁹ As the distinction between public and private spheres erodes in the digital environment, data generated in ostensibly private contexts becomes available for state access and

⁶ Y. Zhu, "Privacy cynicism and diminishing utility of state surveillance," *Big Data & Society* 11, no. 2 (2024), <https://doi.org/10.1177/20539517241242450>.

⁷ I. Zempi dan A. Tripli, "Listening to Muslim students' voices on the Prevent Duty in British universities: A qualitative study," *Education, Citizenship and Social Justice* 18, no. 2 (2022): 230–45, <https://doi.org/10.1177/17461979221077990>.

⁸ Meireles, "Digital rights in perspective: The evolution of the debate in the Internet Governance Forum"; Riemer dan Peter, "Algorithmic audiencing: Why we need to rethink free speech on social media."

⁹ Riemer dan Peter, "Algorithmic audiencing: Why we need to rethink free speech on social media."

analysis.¹⁰ This erosion challenges classical privacy frameworks grounded in spatial and contextual separations.

The human rights implications of surveillance ecosystems are profound. Privacy, widely recognized as a foundational right under international instruments such as Article 17 of the ICCPR and Article 8 of the European Convention on Human Rights, is directly implicated.¹¹¹² Privacy functions as a precondition for freedom of expression and democratic participation; unconstrained surveillance threatens intellectual autonomy and freedom of thought.¹³ Empirical evidence illustrates the normalization of surveillance and the emergence of “privacy cynicism,” whereby individuals become apathetic toward pervasive monitoring.¹⁴ This normalization risks undermining democratic accountability by weakening citizens’ willingness to assert their rights.

The chilling effect represents one of the most documented consequences of surveillance. Individuals who perceive themselves to be monitored frequently self-censor speech, research, and associations.¹⁵ Empirical studies demonstrate that reminders of governmental monitoring capacity significantly reduce citizens’ willingness to express opinions, even in consolidated democracies.¹⁶

¹⁰ Meireles, “Digital rights in perspective: The evolution of the debate in the Internet Governance Forum.”

¹¹ B. Petkova, “Privacy as Europe’s first amendment,” *European Law Journal* 25, no. 2 (2019): 140–54, <https://doi.org/10.1111/eulj.12316>.

¹² M. Mashendra dkk., “Study of the Implementation Restoration Concept in the Criminal Justice System in Indonesia,” *SASI*, no. Query date: 2026-02-22 22:02:03 (2024).

¹³ Petkova, “Privacy as Europe’s first amendment.”

¹⁴ Zhu, “Privacy cynicism and diminishing utility of state surveillance.”

¹⁵ J. Penney, “Chilling effects and transatlantic privacy,” *European Law Journal* 25, no. 2 (2019): 122–39, <https://doi.org/10.1111/eulj.12315>.

¹⁶ Kristine Eck dkk., “Evade and deceive? Citizen responses to surveillance,” *The Journal of Politics* 83, no. 4 (2021): 1545–58, <https://doi.org/10.1086/715073>.

Research on journalists and writers similarly reveals reluctance to pursue sensitive topics due to fears of surveillance and reprisal.¹⁷ In academic settings, surveillance measures such as the Prevent Duty have been shown to curb political engagement and reinforce feelings of vulnerability among targeted communities.¹⁸ Such chilling effects undermine not only individual expression but the structural conditions necessary for democratic deliberation.

Due process and non-discrimination concerns further complicate the governance of surveillance technologies.¹⁹ The political asymmetry observed in China's location disclosure system illustrates discriminatory deployment patterns.²⁰ Similarly, the disproportionate impact of Prevent on Muslim students reflects the creation of a "suspect community," raising concerns about institutionalized discrimination.²¹ Surveillance technologies can therefore generate collective harms that extend beyond individual privacy violations, implicating broader principles of equality and fairness.

Despite the existence of comprehensive frameworks such as the GDPR, the EU Law Enforcement Directive, and the emerging EU AI

¹⁷ A. Masferrer, "The decline of freedom of expression and social vulnerability in Western democracy," *International Journal for the Semiotics of Law* 36, no. 4 (2023): 1443–75, <https://doi.org/10.1007/s11196-023-09990-1>.

¹⁸ Zempi dan Tripli, "Listening to Muslim students' voices on the Prevent Duty in British universities: A qualitative study."

¹⁹ WO Zamrud dan S. Salam, "Human right and indigenous peoples: Transitional justice approach," ... *Journal of Scientific Research in Science* ..., no. Query date: 2026-02-22 22:02:03 (2022), <https://www.academia.edu/download/90888522/9817.pdf>.

²⁰ Zhu, "Privacy cynicism and diminishing utility of state surveillance."

²¹ Zempi dan Tripli, "Listening to Muslim students' voices on the Prevent Duty in British universities: A qualitative study."

Act, significant regulatory gaps persist.²² International human rights instruments were developed in an analogue era and lack the specificity required to govern technologically complex systems.²³ Even advanced regulatory models face challenges of concretization, individualism, and effective post-deployment oversight.²⁴ Proportionality and necessity principles, traditionally applied to discrete surveillance measures, struggle to address mass data aggregation, algorithmic profiling, and temporal complexity. Existing assessments are often static and reactive, failing to capture the evolving risks generated throughout the data lifecycle.

These conceptual and structural gaps highlight the inadequacy of point-in-time human rights evaluations. Surveillance technologies are dynamic systems whose impacts unfold across stages of data collection, storage, analysis, sharing, and deletion. Aggregated datasets can reveal sensitive insights long after initial collection, challenging traditional proportionality analysis.²⁵ Moreover, the concentration of technical expertise within private corporations complicates transparency and democratic oversight, reinforcing concerns about corporate capture and digital colonialism.²⁶

²² Qingxiu Bu, "The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges," *International Cybersecurity Law Review* 2, no. 1 (2021): 113–45, <https://doi.org/10.1365/s43439-021-00022-x>; Petkova, "Privacy as Europe's first amendment."

²³ D. Bunikowski dan P. Dillon, "Arguments from Cultural Ecology and Legal Pluralism for Recognising Indigenous Customary Law in the Arctic," dalam *Springer Polar Sci.* (Springer Nature, 2017), 37–64, Scopus, https://doi.org/10.1007/978-3-319-48069-5_4.

²⁴ R. Sandall, "What Native Peoples Deserve," *Commentary* 119, no. 5 (2005): 54–59, Scopus.

²⁵ Meireles, "Digital rights in perspective: The evolution of the debate in the Internet Governance Forum."

²⁶ Kwet, "Digital colonialism: US empire and the new imperialism in the Global South."

In light of these challenges, this study proposes a dynamic, lifecycle-based human rights risk assessment model tailored to surveillance ecosystems and offers a distinct contribution when compared with five strands of previous scholarship. First, Kosta's study on algorithmic state surveillance provides an important human rights critique by questioning the notion of agency in algorithmic monitoring and by showing how automated surveillance may weaken individual autonomy and accountability. However, that study primarily focuses on the conceptual tension between agency and state surveillance, without developing an operational model that guides law enforcement institutions in assessing risks across the full lifecycle of data processing. The novelty of this article lies in translating such human rights concerns into a structured assessment mechanism that can be applied from data collection to deletion and systemic review. Second, Bu's research on automated facial recognition offers a valuable analysis of ethical, legal, and privacy challenges arising from biometric surveillance. While that work contributes significantly to the governance debate on facial recognition, its focus remains largely technology-specific. By contrast, the present study develops a broader framework applicable not only to automated facial recognition but also to predictive policing,

biometric databases, algorithmic profiling, cross-agency data integration, and other forms of big data-based law enforcement surveillance. Third, Bennett and Raab's work on privacy governance provides a strong foundation for understanding contemporary privacy policy instruments and regulatory challenges. Nevertheless, their analysis is mainly situated within the broader governance of privacy and does not specifically construct a human rights risk assessment tool for law enforcement surveillance ecosystems. This article advances that discussion by integrating privacy governance with the principles of necessity, proportionality, transparency, accountability, non-discrimination, and independent oversight in a lifecycle-based model. Fourth, Amicelle's study on big data surveillance across policing and regulatory fields demonstrates how algorithmic governance operates across institutional domains and produces new forms of power and control. However, that study is more descriptive and analytical in explaining the expansion of big data surveillance, whereas this article moves further by proposing a normative-operational framework designed to evaluate, mitigate, and review human rights risks generated by such surveillance practices. Fifth, Sloane and Wüllhorst's systematic review of transparency mandates in AI regulation identifies regulatory strategies in Europe, the United States, and Canada and highlights the limits of transparency as a governance mechanism. The present study builds on this insight but argues that transparency alone is insufficient unless it is connected to contestability, proportionality review, algorithmic auditing, retention limits, deletion duties, and independent oversight. Accordingly, the novelty of this article is not merely the identification of surveillance risks, but the formulation of the Dynamic Human Rights Risk Assessment Model (DHRRAM) as an integrated governance framework. DHRRAM differs from

previous studies in three principal ways. First, it is lifecycle-based, meaning that human rights protection is embedded at every stage of surveillance data processing, including collection, storage, analysis, sharing, deletion, and systemic review. Second, it is dynamic and adaptive, requiring periodic reassessment as technologies, datasets, institutional uses, and social impacts evolve over time. Third, it is operational rather than purely conceptual, because it links each stage of the surveillance lifecycle with concrete safeguards such as pre-deployment human rights impact assessments, algorithmic bias testing, auditable transfer trails, retention schedules, sunset clauses, and independent oversight. Through this contribution, the article bridges the gap between abstract human rights principles and the practical governance needs of technologically mediated law enforcement. It therefore contributes to legal scholarship, technology governance, and human rights studies by offering a model that is capable of addressing regulatory fragmentation, algorithmic opacity, and static compliance failures in contemporary surveillance ecosystems.

Drawing upon the concept of end-to-end data responsibility and decision provenance, the model evaluates human rights implications at each stage of the data lifecycle. By integrating comparative legal analysis with principle-based technology governance, it seeks to operationalize proportionality, necessity, transparency, and accountability in a structured yet adaptive manner.²⁷ Such a framework moves beyond static compliance toward continuous

²⁷ Bu, "The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges"; C. Sanders dan K. Burnett, "A Case Study in Personal Identification and Social Determinants of Health: Unregistered Births among Indigenous People in Northern Ontario," *International Journal of Environmental Research and Public Health* 16, no. 4 (2019), Scopus, <https://doi.org/10.3390/ijerph16040567>.

oversight, embedding human rights assessment within the architecture of surveillance systems themselves.

Accordingly, this study is guided by the following research question: how can human rights protection be operationalized across the lifecycle of surveillance technology and big data-based law enforcement to ensure proportionality, necessity, transparency, and accountability amid rapid technological change? In answering this question, the article aims to bridge the gap between abstract normative commitments and the complex realities of technologically mediated law enforcement by proposing a governance model capable of safeguarding fundamental rights while adapting to technological innovation.,

II. METHODS

This research adopts a qualitative normative-empirical design to examine the intersection of human rights law and surveillance technology governance. This research adopts a qualitative normative-empirical and socio-legal design to examine the intersection between human rights law and surveillance technology governance. The normative component is used to analyze the legal principles, doctrines, and standards that regulate surveillance practices, particularly the principles of legality, necessity, proportionality, transparency, accountability, non-discrimination, and access to remedy. This component focuses on the interpretation of international and regional human rights instruments, including the ICCPR and the ECHR, as well as relevant data protection and technology governance frameworks that shape the legality of surveillance-based law enforcement. Through doctrinal legal analysis, the study evaluates whether existing rules provide sufficient safeguards against privacy intrusion, algorithmic opacity,

discriminatory profiling, and excessive data retention. The empirical dimension does not rely on field interviews or quantitative surveys, but on qualitative empirical materials derived from documented regulatory practices, case studies, policy reports, jurisprudence, and scholarly findings concerning the use of surveillance technologies in law enforcement. This dimension enables the study to examine how legal norms operate in practice and how surveillance systems generate risks across different institutional and technological contexts. In this sense, the normative-empirical approach allows the research to move beyond abstract legal analysis by connecting human rights principles with concrete governance problems arising from automated facial recognition, predictive policing, cross-agency data sharing, biometric databases, and algorithmic risk assessment tools. The socio-legal approach further strengthens the analysis by situating law within its broader social, institutional, and technological environment. Surveillance technology is not treated merely as a technical instrument or a neutral law enforcement tool, but as part of a wider governance ecosystem involving state agencies, private technology providers, regulatory institutions, databases, algorithms, and affected communities. The socio-legal perspective therefore examines how power relations, institutional capacity, regulatory fragmentation, technical opacity, and public-private cooperation influence the protection or erosion of human rights. This approach is particularly important because surveillance harms often arise not only from formal legal violations, but also from systemic practices such as normalization of monitoring, chilling effects on expression, discriminatory targeting, and limited contestability of automated decisions. The analysis was conducted in several stages. First, the study identified relevant human rights norms applicable to surveillance and big data law enforcement. Second, it reviewed

regulatory frameworks governing data protection, algorithmic governance, and law enforcement surveillance. Third, it examined selected examples and documented controversies to identify recurring governance failures. Fourth, it compared regulatory responses across different jurisdictions to assess fragmentation, oversight deficits, and enforcement limitations. Finally, the findings were synthesized to develop the Dynamic Human Rights Risk Assessment Model, which operationalizes human rights protection across the surveillance data lifecycle, from data collection and storage to processing, sharing, deletion, and systemic review.

This research adopts a qualitative normative-empirical design to examine the intersection of human rights law and surveillance technology governance through a structured step-by-step analysis: first, identifying relevant international and regional human rights norms; second, reviewing legal and regulatory frameworks governing surveillance technologies; third, comparing selected jurisdictional approaches; fourth, examining documented surveillance controversies as illustrative cases; and finally, synthesizing these findings to construct a dynamic human rights risk assessment model.

The methodological framework combines doctrinal legal research, comparative legal analysis, and regulatory theory to construct a dynamic human rights risk assessment model. Doctrinal analysis provides the normative foundation by systematically interpreting international and regional human rights instruments, including the ICCPR and the ECHR, as well as statutory frameworks governing surveillance technologies.²⁸ Through close reading of jurisprudence

²⁸ Shouvik Chatterjee dan S. N.S., "Artificial intelligence and human rights: A comprehensive study from Indian legal and policy perspective," *International Journal of Law and Management* 64,

and legislative texts, the study evaluates how principles such as proportionality, necessity, legality, and accountability are articulated and applied in technologically complex contexts.²⁹

Comparative legal analysis further examines regulatory divergences and convergences across jurisdictions, particularly within the European Union, the United States, and selected Asian legal systems. Comparative scholarship demonstrates that privacy protections and oversight mechanisms vary significantly, resulting in fragmented governance and inconsistent safeguards.³⁰ By identifying best practices and structural weaknesses, the comparative approach enables normative synthesis and highlights gaps in addressing extraterritorial and algorithmic surveillance.³¹ The research also draws upon socio-legal and critical interdisciplinary perspectives to situate legal norms within broader political and technological contexts.³² Building on principle-based governance and regulatory

no. 1 (2021): 110–34, <https://doi.org/10.1108/ijlma-02-2021-0049>; E. Kosta, “Algorithmic state surveillance: Challenging the notion of agency in human rights,” *Regulation & Governance* 16, no. 1 (2020): 212–24, <https://doi.org/10.1111/rego.12331>.

²⁹ Quirine Eijkman, “Access to justice for communications surveillance and interception: Scrutinising intelligence-gathering reform legislation,” *Utrecht Law Review* 14, no. 1 (2018): 116, <https://doi.org/10.18352/ulr.419>; J. Marson, M. White, dan K. Ferris, “The Investigatory Powers Act 2016 and connected vehicles,” *Statute Law Review* 44, no. 1 (2022), <https://doi.org/10.1093/slr/hmac004>.

³⁰ Bu, “The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges”; Y. Shany, “Catching up: The European Court of Human Rights approximates its approach to extraterritorial jurisdiction over digital surveillance,” *The European Convention on Human Rights Law Review*, advance online publication, 2024, <https://doi.org/10.1163/26663236-bja10089>.

³¹ M. Rojszczak, “Extraterritorial bulk surveillance after the German BND Act judgment,” *European Constitutional Law Review* 17, no. 1 (2021): 53–77, <https://doi.org/10.1017/s1574019621000055>.

³² Colin Bennett dan Charles Raab, “Revisiting the governance of privacy: Contemporary policy instruments in global perspective,” *Regulation & Governance* 14, no. 3 (2018): 447–64, <https://doi.org/10.1111/rego.12222>; Thiago DoCarmo dkk., “The law in computation: What

theory, the study develops a dynamic human rights risk assessment model grounded in proportionality, non-discrimination, transparency, and continuous oversight.³³ Rather than relying on static compliance assessments, the model maps potential risks across the surveillance data lifecycle and integrates adaptive monitoring mechanisms. Through document analysis, regulatory review, and case studies of documented surveillance controversies, the methodology identifies normative gaps and formulates a structured yet flexible governance framework capable of responding to evolving technological risks.

III. RESULT AND DISCUSSION

A. Structural Deficiencies in Existing Surveillance Governance Frameworks

The analysis confirms that existing regulatory frameworks governing surveillance technology and big data law enforcement are marked by deep structural weaknesses and systemic fragmentation. These weaknesses are multidimensional and mutually reinforcing, operating across jurisdictional, institutional, conceptual, and temporal levels. Three primary deficiencies stand out: fragmented oversight mechanisms, insufficient transparency in algorithmic decision-making, and the absence of contextual proportionality assessment throughout the data lifecycle. Three primary deficiencies stand out: fragmented oversight mechanisms, insufficient

machine learning, artificial intelligence, and big data mean for law and society scholarship," *Law & Policy* 43, no. 2 (2021): 170–99, <https://doi.org/10.1111/lapo.12164>.

³³ Andreas Fischer-Lescano, "Struggles for a global Internet constitution: Protecting global communication structures against surveillance measures," *Global Constitutionalism* 5, no. 2 (2016): 145–72, <https://doi.org/10.1017/s204538171600006x>; O. Ugwu dkk., "Harnessing technology for infectious disease response in conflict zones," *Medicine* 103, no. 28 (2024): e38834, <https://doi.org/10.1097/md.00000000000038834>.

transparency in algorithmic decision-making, and the absence of contextual proportionality assessment throughout the data lifecycle. For example, the use of automated facial recognition in public policing may simultaneously fall under data protection law, criminal procedure, AI governance rules, and national security regulations, yet no single oversight body may possess full authority to assess its cumulative human rights impact. Similarly, predictive policing systems can generate risk scores from historical crime data without clearly disclosing how variables are weighted, making it difficult for affected individuals to challenge biased or inaccurate outcomes. These examples illustrate how fragmented regulation and algorithmic opacity can weaken meaningful accountability in surveillance-based law enforcement.

These shortcomings are embedded within what regulatory scholarship identifies as the “pacing problem,” namely the structural lag between technological innovation and regulatory adaptation.³⁴ AI-driven surveillance systems—characterized by opacity, autonomy, and systemic risk—have evolved more rapidly than the legal doctrines designed to constrain them, exposing the limitations of static, principle-based regulation when confronted with adaptive algorithmic infrastructures.³⁵

³⁴ Wendy Currie dkk., “Rethinking technology regulation in the age of AI risks,” *Journal of Information Technology* 40, no. 3 (2025): 236–45, <https://doi.org/10.1177/02683962251378815>.

³⁵ Currie dkk., “Rethinking technology regulation in the age of AI risks”; G. Oatley, “Themes in data mining, big data, and crime analytics,” *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 12, no. 2 (2021), <https://doi.org/10.1002/widm.1432>.

Fragmentation is visible first at the jurisdictional level. The absence of a comprehensive global legal framework governing surveillance technology has produced uneven standards of protection and opportunities for regulatory arbitrage.³⁶ Divergences between regional regimes, such as the GDPR-based European model and more sectoral or security-driven frameworks elsewhere, create inconsistencies in safeguards, enforcement capacity, and accountability mechanisms. Even within the European Union, regulatory complexity persists at the interface between the GDPR, the Law Enforcement Directive, and the AI Act, generating ambiguities in competence allocation and procedural rights.^{37,38} The result is structural incoherence, where surveillance practices transcend jurisdictional boundaries while accountability remains territorially constrained.

Fragmentation also operates across regulatory domains. Surveillance practices simultaneously implicate data protection law, criminal procedure law, national security law, competition regulation, and human rights law, yet these domains remain institutionally siloed.³⁹

³⁶ O. Gstrein, "Mapping power and jurisdiction on the internet through the lens of government-led surveillance," *Internet Policy Review*, advance online publication, 2020, <https://doi.org/10.14763/2020.3.1497>; V. Mone dkk., "Data warfare and creating a global legal and regulatory landscape: Challenges and solutions," *International Journal of Legal Information* 52, no. 2 (2024): 124–34, <https://doi.org/10.1017/jli.2024.22>.

³⁷ M. Wörsdörfer, "Mitigating the adverse effects of AI with the European Union's Artificial Intelligence Act: Hype or hope?," *Global Business and Organizational Excellence* 43, no. 3 (2023): 106–26, <https://doi.org/10.1002/joe.22238>.

³⁸ J. Mazur dan R. Włoch, "Embedding digital economy: Fictitious triple movement in the European Union's Artificial Intelligence Act," *Social & Legal Studies* 33, no. 1 (2023): 104–23, <https://doi.org/10.1177/09646639231152866>; Wörsdörfer, "Mitigating the adverse effects of AI with the European Union's Artificial Intelligence Act: Hype or hope?"

³⁹ P. Keller, "The reconstruction of privacy through law: A strategy of diminishing expectations," *International Data Privacy Law* 9, no. 3 (2019): 132–52, <https://doi.org/10.1093/idpl/ipz012>; P. Popiel, "Regulating datafication and platformization: Policy silos and tradeoffs in international platform inquiries," *Policy & Internet* 14, no. 1 (2022): 28–46, <https://doi.org/10.1002/poi3.283>.

Policy area silos prevent holistic assessment of surveillance harms, as each regulatory regime addresses only a subset of risks. The proliferation of surveillance intermediaries and hybrid public-private arrangements further disperses responsibility, reducing transparency and diffusing legal liability.⁴⁰

A second structural weakness lies in insufficient transparency and contestability in algorithmic decision-making. Data-driven law enforcement increasingly relies on predictive analytics and automated facial recognition systems whose operational logic remains opaque to affected individuals and even oversight authorities.⁴¹ Disclosure mandates frequently fail to translate into meaningful accountability due to technical complexity, trade secrecy claims, and institutional asymmetries of expertise.⁴² Without procedural rights enabling individuals to challenge automated outputs, transparency risks becoming symbolic rather than transformative.⁴³ A third deficiency concerns the absence of contextual proportionality assessment across the data lifecycle. Most regulatory frameworks emphasize compliance at the point of data collection yet neglect downstream risks such as predictive profiling,

⁴⁰ Anthony Amicelle, "Big data surveillance across fields: Algorithmic governance for policing & regulation," *Big Data & Society* 9, no. 2 (2022), <https://doi.org/10.1177/20539517221112431>; T. Riebedick, "U.S. security policy: The dual-use regulation of cryptography and its effects on surveillance," *European Journal for Security Research* 7, no. 1 (2022): 39–65, <https://doi.org/10.1007/s41125-022-00080-0>.

⁴¹ Keller, "The reconstruction of privacy through law: A strategy of diminishing expectations"; Oatley, "Themes in data mining, big data, and crime analytics."

⁴² Curriedick, "Rethinking technology regulation in the age of AI risks"; M. Sloane and E. Wüllhorst, "A systematic review of regulatory strategies and transparency mandates in AI regulation in Europe, the United States, and Canada," *Data & Policy* 7 (2025), <https://doi.org/10.1017/dap.2024.54>.

⁴³ Mazur and Włoch, "Embedding digital economy: Fictitious triple movement in the European Union's Artificial Intelligence Act."

cross-agency integration, and indefinite retention.⁴⁴ Surveillance harms often materialize during aggregation and analysis, when individually innocuous data points are transformed into behavioral predictions.⁴⁵ Static assessments at a single procedural juncture cannot adequately capture the evolving risk landscape of algorithmic surveillance. Enforcement deficits compound these structural weaknesses. Regulatory agencies frequently lack the technical expertise and institutional resources necessary to audit complex systems effectively.⁴⁶ Fragmented enforcement across jurisdictions further dilutes accountability, producing a governance environment in which surveillance technologies proliferate rapidly while oversight remains reactive and procedurally constrained.

B. Operationalization of the Dynamic Human Rights Risk Assessment Model (DHRRAM)

In response to these systemic shortcomings, this study advances the Dynamic Human Rights Risk Assessment Model (DHRRAM), a lifecycle-based governance framework designed to embed proportionality, necessity, transparency, and accountability at each stage of surveillance data processing.

⁴⁴ Bu, "The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges"; Keller, "The reconstruction of privacy through law: A strategy of diminishing expectations."

⁴⁵ Oatley, "Themes in data mining, big data, and crime analytics."

⁴⁶ Currie dkk., "Rethinking technology regulation in the age of AI risks."

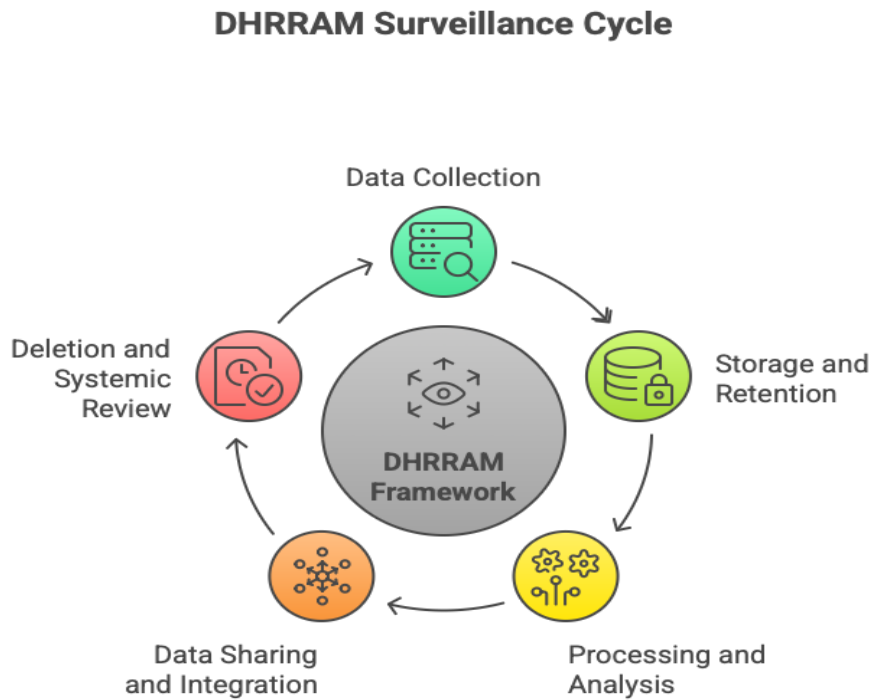


Figure 1. DHRRAM Surveillance Cycle

As illustrated in Figure 1, DHRRAM operates through five interconnected stages—data collection, storage and retention, processing and analysis, sharing and integration, and deletion and systemic review—each requiring specific safeguards, including human rights impact assessment, periodic necessity review, algorithmic auditing, auditable transfer trails, sunset clauses, and independent oversight. Figure 1 illustrates the Dynamic Human Rights Risk Assessment Model (DHRRAM) as a lifecycle-based governance framework for surveillance technology and big data law enforcement. The model shows that human rights protection should not be treated as a one-time compliance requirement, but as a continuous process embedded across the entire surveillance data lifecycle. The framework begins at the data collection stage, where surveillance activities must be justified by clear necessity, lawful purpose, and proportionality. Before data is collected, institutions should conduct a human rights impact assessment, define the specific

purpose of surveillance, and obtain independent authorization where required. The second stage concerns storage and retention. At this point, DHRRAM requires secure storage, purpose-specific retention periods, periodic necessity reviews, and mandatory deletion protocols. These safeguards prevent indefinite data retention and reduce the risk that collected information will be reused beyond its original lawful purpose. The third stage is processing and analysis, where the greatest risks often arise from predictive analytics, automated facial recognition, algorithmic profiling, and other AI-based tools. DHRRAM requires algorithmic impact assessments, bias testing, error-rate evaluation, human-in-the-loop review, and mechanisms that allow affected individuals to contest automated or data-driven decisions. The fourth stage addresses data sharing and integration, especially when information is transferred between agencies, jurisdictions, or public-private actors. The model emphasizes contextual proportionality tests, auditable transfer trails, strict necessity thresholds, and accountability mechanisms to prevent regulatory arbitrage, excessive data circulation, and opaque inter-agency surveillance practices. The final stage is deletion and systemic review. DHRRAM requires sunset clauses, lifecycle audits, independent evaluation, and adaptive reassessment of emerging risks. This ensures that surveillance systems remain subject to ongoing review even after deployment and that obsolete, unlawful, or disproportionate systems can be modified or terminated. Figure 1 demonstrates that DHRRAM transforms surveillance governance from episodic compliance into adaptive human rights stewardship. By integrating necessity, proportionality, transparency, accountability, and non-discrimination across every stage of the data lifecycle, the model provides a structured yet flexible framework for

protecting fundamental rights in technologically mediated law enforcement.

The core insight of DHRRAM is that surveillance risks evolve temporally and institutionally; therefore, governance must be continuous rather than episodic. At the data collection stage, DHRRAM requires rigorous necessity justification and predefined purpose limitation. Pre-collection impact assessments, publicly accessible surveillance use policies, and independent authorization mechanisms ensure that the threshold for intrusion is substantively justified.⁴⁷

During storage and retention, the model introduces purpose-specific retention schedules, mandatory deletion protocols, and periodic necessity reviews to operationalize proportionality beyond the initial collection phase (Keller, 2019). Security audits and breach notification requirements address systemic vulnerabilities in large-scale databases.⁴⁸ At the processing and analysis stage, DHRRAM mandates algorithmic impact assessments evaluating error rates, disparate impacts, and systemic bias prior to deployment and at regular intervals thereafter.⁴⁹ Independent audits, red-teaming exercises, and human-in-the-loop safeguards enhance contestability and mitigate overreliance on opaque computational reasoning.⁵⁰

⁴⁷ Bu, “The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges”; Sloane dan Wüllhorst, “A systematic review of regulatory strategies and transparency mandates in AI regulation in Europe, the United States, and Canada.”

⁴⁸ Mone dkk., “Data warfare and creating a global legal and regulatory landscape: Challenges and solutions.”

⁴⁹ Bu, “The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges.”

⁵⁰ Amicelle, “Big data surveillance across fields: Algorithmic governance for policing & regulation”; Sloane dan Wüllhorst, “A systematic review of regulatory strategies and transparency mandates in AI regulation in Europe, the United States, and Canada.”

For data sharing and cross-agency integration, the model introduces contextual proportionality tests governing transfers, strict necessity thresholds for cross-border exchanges, and auditable decision trails to prevent regulatory arbitrage and opacity in multi-actor ecosystems.⁵¹ Finally, at the deletion and systemic review stage, DHRRAM incorporates sunset clauses, lifecycle audits, and periodic independent evaluations. By mandating adaptive reassessment in light of technological evolution, the model directly addresses the pacing problem and transforms oversight from episodic judicial intervention into structured, ongoing governance. In sum, the results demonstrate that existing surveillance governance frameworks are structurally ill-equipped to manage the complexity of big data law enforcement. Fragmentation, opacity, enforcement deficits, and static proportionality assessments collectively undermine effective human rights protection. The Dynamic Human Rights Risk Assessment Model offers a structured yet adaptive alternative, embedding core principles across the entire data lifecycle and transforming surveillance governance from episodic regulation into continuous human rights stewardship.

VI. CONCLUSION

The integration of surveillance technology and big data analytics into law enforcement creates a governance dilemma: while these tools may enhance efficiency, prediction, and public security, they also generate serious risks to privacy, non-discrimination, due process, and democratic accountability. This study has shown that existing regulatory frameworks remain fragmented across jurisdictions and

⁵¹ Currie dkk., "Rethinking technology regulation in the age of AI risks"; Gstrein, "Mapping power and jurisdiction on the internet through the lens of government-led surveillance."

regulatory domains, insufficiently adaptive to technological change, and overly dependent on static compliance mechanisms. Such limitations prevent current governance models from adequately addressing the lifecycle-based risks that emerge during data collection, storage, processing, sharing, and deletion.

To address these problems, this study advances the Dynamic Human Rights Risk Assessment Model (DHRRAM) as a lifecycle-based framework for continuous human rights governance in surveillance-based law enforcement. By embedding necessity, proportionality, transparency, accountability, and non-discrimination across each stage of the surveillance data lifecycle, the model shifts oversight from reactive compliance to adaptive human rights stewardship. The proposed framework contributes to legal and technology governance scholarship by translating human rights principles into operational safeguards, including impact assessments, algorithmic auditing, retention review, auditable data-sharing mechanisms, sunset clauses, and independent oversight. Future research should empirically test the model across specific national and regional contexts to assess its practical feasibility and effectiveness in protecting fundamental rights amid rapidly evolving surveillance ecosystems.

ACKNOWLEDGMENTS

Thank you to the author's friends in this paper who have contributed to this paper. May this writing be a writing that begins our other writings

REFERENCES

Amicelle, Anthony. "Big data surveillance across fields: Algorithmic governance for policing & regulation." *Big Data & Society* 9, no. 2 (2022). <https://doi.org/10.1177/20539517221112431>.

Bennett, Colin, dan Charles Raab. "Revisiting the governance of privacy: Contemporary policy instruments in global perspective." *Regulation & Governance* 14, no. 3 (2018): 447–64. <https://doi.org/10.1111/rego.12222>.

Bu, Qingxiu. "The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges." *International Cybersecurity Law Review* 2, no. 1 (2021): 113–45. <https://doi.org/10.1365/s43439-021-00022-x>.

Bunikowski, D., dan P. Dillon. "Arguments from Cultural Ecology and Legal Pluralism for Recognising Indigenous Customary Law in the Arctic." Dalam *Springer Polar Sci.*, 37–64. Springer Nature, 2017. Scopus. https://doi.org/10.1007/978-3-319-48069-5_4.

Chatterjee, Shouvik, dan S. N.S. "Artificial intelligence and human rights: A comprehensive study from Indian legal and policy perspective." *International Journal of Law and Management* 64, no. 1 (2021): 110–34. <https://doi.org/10.1108/ijlma-02-2021-0049>.

Currie, Wendy, Daniel Schlagwein, Jan Leimeister, dan Leslie Willcocks. "Rethinking technology regulation in the age of AI risks." *Journal of Information Technology* 40, no. 3 (2025): 236–45. <https://doi.org/10.1177/02683962251378815>.

DoCarmo, Thiago, Samuel Rea, Emily Conaway, Jessica Emery, dan Noopur Raval. "The law in computation: What machine learning, artificial intelligence, and big data mean for law and society scholarship." *Law & Policy* 43, no. 2 (2021): 170–99. <https://doi.org/10.1111/lapo.12164>.

Eck, Kristine, Samuel Hatz, Charles Crabtree, dan Atsushi Tago. "Evade and deceive? Citizen responses to surveillance." *The*

Journal of Politics 83, no. 4 (2021): 1545–58.
<https://doi.org/10.1086/715073>.

Eijkman, Quirine. “Access to justice for communications surveillance and interception: Scrutinising intelligence-gathering reform legislation.” *Utrecht Law Review* 14, no. 1 (2018): 116.
<https://doi.org/10.18352/ulr.419>.

Fischer-Lescano, Andreas. “Struggles for a global Internet constitution: Protecting global communication structures against surveillance measures.” *Global Constitutionalism* 5, no. 2 (2016): 145–72. <https://doi.org/10.1017/s204538171600006x>.

Gstrein, O. “Mapping power and jurisdiction on the internet through the lens of government-led surveillance.” *Internet Policy Review*, advance online publication, 2020.
<https://doi.org/10.14763/2020.3.1497>.

Keller, P. “The reconstruction of privacy through law: A strategy of diminishing expectations.” *International Data Privacy Law* 9, no. 3 (2019): 132–52. <https://doi.org/10.1093/idpl/ipz012>.

Kosta, E. “Algorithmic state surveillance: Challenging the notion of agency in human rights.” *Regulation & Governance* 16, no. 1 (2020): 212–24. <https://doi.org/10.1111/regg.12331>.

Kwet, M. “Digital colonialism: US empire and the new imperialism in the Global South.” *Race & Class* 60, no. 4 (2019): 3–26.
<https://doi.org/10.1177/0306396818823172>.

Marson, J., M. White, dan K. Ferris. “The Investigatory Powers Act 2016 and connected vehicles.” *Statute Law Review* 44, no. 1 (2022).
<https://doi.org/10.1093/slr/hmac004>.

Masferrer, A. “The decline of freedom of expression and social vulnerability in Western democracy.” *International Journal for the*

Semiotics of Law 36, no. 4 (2023): 1443–75. <https://doi.org/10.1007/s11196-023-09990-1>.

Mashendra, M., KM Ibrahim, S. Salam, E. Nurcahyo, dan ... “Study of the Implementation Restoration Concept in the Criminal Justice System in Indonesia.” *SASI*, no. Query date: 2026-02-22 22:02:03 (2024).

Mazur, J., dan R. Włoch. “Embedding digital economy: Fictitious triple movement in the European Union’s Artificial Intelligence Act.” *Social & Legal Studies* 33, no. 1 (2023): 104–23. <https://doi.org/10.1177/09646639231152866>.

Meireles, A. “Digital rights in perspective: The evolution of the debate in the Internet Governance Forum.” *Politics & Policy* 52, no. 1 (2024): 12–32. <https://doi.org/10.1111/polp.12571>.

Mone, V., S. Abdulajonovich, A. Younas, dan S. Petikam. “Data warfare and creating a global legal and regulatory landscape: Challenges and solutions.” *International Journal of Legal Information* 52, no. 2 (2024): 124–34. <https://doi.org/10.1017/jli.2024.22>.

Oatley, G. “Themes in data mining, big data, and crime analytics.” *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 12, no. 2 (2021). <https://doi.org/10.1002/widm.1432>.

Penney, J. “Chilling effects and transatlantic privacy.” *European Law Journal* 25, no. 2 (2019): 122–39. <https://doi.org/10.1111/eulj.12315>.

Petkova, B. “Privacy as Europe’s first amendment.” *European Law Journal* 25, no. 2 (2019): 140–54. <https://doi.org/10.1111/eulj.12316>.

Popiel, P. “Regulating datafication and platformization: Policy silos and tradeoffs in international platform inquiries.” *Policy & Internet* 14, no. 1 (2022): 28–46. <https://doi.org/10.1002/poi3.283>.

Ricknell, E. "Freedom of expression and alternatives for internet governance: Prospects and pitfalls." *Media and Communication* 8, no. 4 (2020): 110–20. <https://doi.org/10.17645/mac.v8i4.3299>.

Riebe, T., P. Kühn, P. Imperatori, dan C. Reuter. "U.S. security policy: The dual-use regulation of cryptography and its effects on surveillance." *European Journal for Security Research* 7, no. 1 (2022): 39–65. <https://doi.org/10.1007/s41125-022-00080-0>.

Riemer, K., dan S. Peter. "Algorithmic audiencing: Why we need to rethink free speech on social media." *Journal of Information Technology* 36, no. 4 (2021): 409–26. <https://doi.org/10.1177/02683962211013358>.

Rojszczak, M. "Extraterritorial bulk surveillance after the German BND Act judgment." *European Constitutional Law Review* 17, no. 1 (2021): 53–77. <https://doi.org/10.1017/s1574019621000055>.

Sandall, R. "What Native Peoples Deserve." *Commentary* 119, no. 5 (2005): 54–59. Scopus.

Sanders, C., dan K. Burnett. "A Case Study in Personal Identification and Social Determinants of Health: Unregistered Births among Indigenous People in Northern Ontario." *International Journal of Environmental Research and Public Health* 16, no. 4 (2019). Scopus. <https://doi.org/10.3390/ijerph16040567>.

Shany, Y. "Catching up: The European Court of Human Rights approximates its approach to extraterritorial jurisdiction over digital surveillance." *The European Convention on Human Rights Law Review*, advance online publication, 2024. <https://doi.org/10.1163/26663236-bja10089>.

Sloane, M., dan E. Wüllhorst. "A systematic review of regulatory strategies and transparency mandates in AI regulation in Europe, the United States, and Canada." *Data & Policy* 7 (2025). <https://doi.org/10.1017/dap.2024.54>.

Ugwu, O., E. Alum, J. Ugwu, V. Eze, C. Ugwu, F. Ogenyi, dan M. Okon. "Harnessing technology for infectious disease response in conflict zones." *Medicine* 103, no. 28 (2024): e38834. <https://doi.org/10.1097/md.00000000000038834>.

Wörsdörfer, M. "Mitigating the adverse effects of AI with the European Union's Artificial Intelligence Act: Hype or hope?" *Global Business and Organizational Excellence* 43, no. 3 (2023): 106–26. <https://doi.org/10.1002/joe.22238>.

Zamrud, WO, dan S. Salam. "Human right and indigenous peoples: Transitional justice approach." ... *Journal of Scientific Research in Science* ..., no. Query date: 2026-02-22 22:02:03 (2022). <https://www.academia.edu/download/90888522/9817.pdf>.

Zempi, I., dan A. Tripli. "Listening to Muslim students' voices on the Prevent Duty in British universities: A qualitative study." *Education, Citizenship and Social Justice* 18, no. 2 (2022): 230–45. <https://doi.org/10.1177/17461979221077990>.

Zhu, Y. "Privacy cynicism and diminishing utility of state surveillance." *Big Data & Society* 11, no. 2 (2024). <https://doi.org/10.1177/20539517241242450>.