

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

Human Rights and Digital Surveillance in the Era of Smart Governance

Mery Yarni
Jambi University, Jambi, Indonesia

Received: July 11, 2026
Revised: August 6, 2026
Accepted: August 24, 2026
Published: August 28, 2026

Corresponding Author:
Author Name*: Mery Yarni
E-mail*:
yarnimery@gmail.com



Abstract: *The rapid diffusion of smart governance an administrative paradigm that fuses artificial intelligence, big-data analytics, the Internet of Things, and biometric identification into the machinery of public administration has fundamentally reconfigured the relationship between the state and the citizen. While proponents celebrate smart governance as a vehicle for efficiency, transparency, and responsive public service delivery, its infrastructural backbone is inseparable from pervasive digital surveillance: continuous data collection, algorithmic profiling, facial recognition, and predictive analytics deployed by both public authorities and private technology vendors. This article examines the resulting tension between the developmental promise of smart governance and the human rights obligations that bind states under international and domestic law, with particular attention to the rights to privacy, freedom of expression, non-discrimination, and due process. Employing a normative legal method that combines statutory, conceptual, and comparative approaches, the article analyses international human rights instruments, national data-protection legislation including Indonesia's Law No. 27 of 2022 and recent doctrinal literature to map the legal gaps that permit surveillance overreach. The findings indicate that existing legal frameworks remain reactive, fragmented, and structurally ill-equipped to govern the algorithmic and biometric surveillance embedded in smart-city infrastructure. The article concludes that a human-rights-based approach to smart governance design, anchored in proportionality, purpose limitation, transparency, and independent oversight, is indispensable to reconciling technological modernisation with the protection of fundamental rights.*

Keywords: *Human Rights; Digital Surveillance; Smart Governance; Data Protection; Privacy.*

INTRODUCTION

Over the past decade, governments across the globe have embraced the vision of "smart governance" as the organising principle of twenty-first-century public administration. Denmark's digitised welfare bureaucracy, in which eligibility for social benefits is increasingly determined through automated data-matching across tax, health, and employment registries, exemplifies how deeply

data-driven decision-making has penetrated the machinery of the state ¹. Indonesia has pursued a parallel trajectory through its Sistem Pemerintahan Berbasis Elektronik (electronic-based government system) and a growing number of municipal "smart city" initiatives, which promise integrated, technology-enabled public services but simultaneously expand the state's capacity to observe, record, and analyse the everyday lives of its citizens ². What unites

¹ R Jørgensen, "Data and Rights in the Digital Welfare State: The Case of Denmark," *Information, Communication & Society* 26 (2021): 123, <https://doi.org/10.1080/1369118x.2021.1934069>.

² M Ananda and A Ikraam, "Perlindungan Hak Asasi Manusia Pada Era Pengawasan Digital

Oleh Negara: Analisis Hukum Tentang Privasi Vs Keamanan," *Jurnal Locus Penelitian dan Pengabdian* (2026), <https://doi.org/10.58344/locus.v5i1.5459>.

these otherwise disparate national experiences is a shared administrative logic: governance is increasingly performed through sensors, algorithms, and databases rather than through discretionary human judgment alone.

Smart governance is commonly defined as the application of information and communication technologies — artificial intelligence, the Internet of Things, cloud computing, and biometric identification — to the design and delivery of public services, urban management, and regulatory enforcement. Its declared objectives are efficiency, transparency, and responsiveness. Yet the very technologies that make governance "smart" are, by design, technologies of observation. Closed-circuit television networks linked to facial recognition, environmental and mobility sensors embedded in urban infrastructure, and centralised biometric identity databases together constitute a surveillance architecture that operates continuously and largely invisibly to those it monitors ³. Recent scholarship guest-edited under the rubric of "future-proofing the city" has shown that the human rights implications of algorithmic and biometric smart-city technologies cut across disciplinary boundaries and demand an integrated legal response rather than piecemeal sectoral regulation ⁴.

The tension this generates is not merely technical but constitutional in character. Scholars of technology and human rights law

have long observed that new surveillance capacities tend to outpace the legal frameworks designed to constrain state power ⁵. Digital surveillance, when untethered from clear legal authorisation, necessity, and proportionality, exposes individuals to risks that reach well beyond the conventional understanding of privacy violations: it can chill political participation, entrench discriminatory policing practices, and erode the very trust between citizen and state that smart governance purports to strengthen ⁶.

The stakes of getting this balance right are not merely doctrinal. Public trust in digital government services depends substantially on citizens' confidence that the data collected in the course of accessing those services will not be repurposed against their interests. Comparative surveys of digital-government adoption consistently find that perceived privacy risk is among the strongest predictors of citizen reluctance to engage with electronic public services, meaning that inadequate rights protection is not only a legal and ethical deficiency but a practical obstacle to the efficiency and service-uptake objectives that motivate smart-governance investment in the first place ⁷. Properly designed rights safeguards should therefore be understood not as a constraint external to the smart-governance project but as a condition of its long-term legitimacy and effectiveness.

³ T Alizadeh and D Prasad, "Smart City Initiatives, Practices and Technologies: Surveillance in Breach of Fundamental Human Rights," *Telematics and Informatics* 106 (2026): 1, <https://doi.org/10.1016/j.tele.2026.102391>.

⁴ A Wernick and A Artyushina, "Future-Proofing the City: A Human Rights-Based Approach to Governing Algorithmic, Biometric and Smart City Technologies," *Internet Policy Review* 12, no. 1 (2023), <https://doi.org/10.14763/2023.1.1695>.

⁵ M Land and J Aronson, "Human Rights and Technology: New Challenges for Justice and

Accountability," *Annual Review of Law and Social Science* (2020), <https://doi.org/10.1146/annurev-lawsocsci-060220-081955>.

⁶ E Talapina, "Surveillance and Human Rights: New Risks in the Digital Age," *Sravnitel'noe konstitucionnoe obozrenie* (2021), <https://doi.org/10.21128/1812-7126-2021-6-123-136>.

⁷ D Georgekutty, "Citizenship in the Digital Age: Rights, Responsibilities, and Surveillance," *International Journal of Social Science Research Studies* (IJSSRS) (2025), <https://doi.org/10.63090/ijssrs/3108.1932.0005>.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

Human rights scholars increasingly describe the harms of pervasive digital surveillance as touching a distinct, evolving category of entitlements. Mathias Risse's account of a "fourth generation" of human rights — epistemic rights concerning what individuals may know, be known as, and reason about, free from covert algorithmic manipulation — captures a dimension of harm that classical privacy doctrine only partially addresses⁸. Similarly, Okonkwo's analysis of the ethical tensions between AI-enabled surveillance architectures and the universal entitlement to digital dignity emphasises that surveillance harms are cumulative and structural, not merely episodic⁹. These accounts converge on a single proposition: the rights implicated by smart governance — privacy, freedom of expression, equality before the law, and due process — are neither peripheral nor speculative but are actively contested in the design choices embedded in today's digital public infrastructure.

The COVID-19 pandemic accelerated this contestation considerably. Public health emergencies provided states with an unprecedented justification to deploy contact-tracing applications, digital health passes, and expanded biometric checkpoints, normalising forms of surveillance that would, in ordinary

circumstances, have faced far greater public and judicial scrutiny¹⁰. Once installed, such infrastructure has rarely been fully dismantled; instead, it has often been repurposed for general law-enforcement and administrative functions, a pattern of "function creep" that is now well documented across both authoritarian and democratic jurisdictions¹¹.

Indonesia's own regulatory response illustrates both the promise and the limits of contemporary efforts to reconcile digital governance with rights protection. The enactment of Law No. 27 of 2022 on Personal Data Protection (Undang-Undang Pelindungan Data Pribadi, hereinafter "the PDP Law") marked a significant step toward a comprehensive domestic data-protection regime¹². Yet doctrinal analysis of the PDP Law's implementation reveals persistent gaps: the absence, at the time of writing, of a fully independent supervisory authority, ambiguity in the law's application to state surveillance conducted in the name of public security, and weak enforcement mechanisms relative to the scale of data processing now embedded in Indonesia's digital public services¹³. These gaps mirror a broader global pattern in which legislative reform, however welcome, consistently lags behind the pace of technological deployment¹⁴.

⁸ M Risse, "The Fourth Generation of Human Rights: Epistemic Rights in Digital Lifeworlds," *Moral Philosophy and Politics* 8 (2021): 351, <https://doi.org/10.1515/mopp-2020-0039>.

⁹ O A Okonkwo, "Ethical Tensions between AI Surveillance Architectures, Human Rights Preservation, and the Universal Entitlement to Digital Privacy and Dignity," *Magna Scientia Advanced Research and Reviews* 9, no. 2 (2023), <https://doi.org/10.30574/msarr.2023.9.2.0179>.

¹⁰ S Sekalala, S Dagron, L Forman, and B Meier, "Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis," *Health and Human Rights* 22, no. 2 (2020): 7, <https://doi.org/10.17615/8e8a-m957>.

¹¹ J Ayan, "The Effect of Digital Surveillance Systems and Their Implications for Civil Liberties in Smart Societies," *Bolan International Journal of Research Insights (BIJRI)* (2026), <https://doi.org/10.66021/bijri.v3i1.41>.

¹² Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

¹³ E Muzairroh, D T Noviasari, and H M Syafingi, "Analisis Perlindungan Hukum Terhadap Privasi Data Pribadi di Era Digital dalam Prespektif Hak Asasi Manusia," *Borobudur Law and Society Journal* 3, no. 1 (2024): 31–36, <https://doi.org/10.31603/11824>.

¹⁴ A Sethi, H H Ullah, and R M S Naseem, "Surveillance, National Security and the Right to

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

These developments carry particular significance for Indonesia's own smart-governance trajectory. As Indonesia's national and municipal governments continue to expand electronic-government platforms, digital identity systems, and municipal smart-city command centres, the country occupies a position shared by many rapidly digitalising states: a legal system in active transition, a data-protection statute of comparatively recent vintage, and an administrative culture accustomed to expanding technological capability more rapidly than the institutional mechanisms required to constrain its use. Examining the international literature on smart governance and digital surveillance is therefore not merely a matter of comparative academic interest; it offers a body of doctrinal experience — both cautionary and constructive — from which Indonesian legal reform can draw as it continues to operationalise the PDP Law and to define the human rights parameters within which its own smart-governance ambitions will be pursued.

Against this backdrop, this article addresses three interrelated questions. First, what is the architecture of digital surveillance embedded within contemporary smart governance, and what administrative, security, and commercial logics drive its expansion? Second, which specific human rights are placed at risk by this architecture, and through what mechanisms do the resulting harms materialise? Third, to what extent do existing international and domestic legal frameworks — including human rights treaties, data-protection statutes, and emerging comparative regulatory models — provide adequate safeguards, and what reforms are necessary to close the identified gaps? The article proceeds as follows. Section two sets out the normative legal method

employed. Section three, divided into two sub-sections, presents the results and discussion: the first sub-section maps the architecture of smart governance and the normalisation of digital surveillance, while the second examines the specific human rights placed at risk and evaluates the adequacy of existing legal safeguards. The article closes with concluding observations and policy recommendations.

This tension is compounded by the global unevenness of regulatory response. Comparative doctrinal work on the age of mass surveillance observes that liberty and security are frequently "recalibrated" by legislatures under conditions of perceived emergency, producing surveillance powers that are formally temporary but, in institutional practice, rarely subject to systematic post-emergency review or sunset enforcement¹⁵. Where such recalibration occurs repeatedly across successive security or public-health crises, the cumulative effect is a steady, largely unreviewed expansion of the state's surveillance capacity, a pattern documented across both established and emerging smart-governance systems¹⁶. This dynamic underscores why the present analysis treats digital surveillance not as a series of discrete policy choices but as a structural feature of the smart-governance paradigm that requires a correspondingly structural — rather than merely incremental — legal response.

The stakes of this inquiry extend beyond the technical design of any single surveillance system to the broader question of what kind of relationship a digitalising state establishes with its citizens. A public administration that can observe, predict, and pre-emptively act upon the behaviour of its population possesses a form of power that classical constitutional theory, built around the separation of powers and

Privacy in the Digital Era," *The Critical Review of Social Sciences Studies* (2025), <https://doi.org/10.59075/gf564d60>.

¹⁵ T Svobodová, "Recalibrating Liberty and Security: Human Rights Challenges in the Age of

Mass Surveillance," *Congress Proceedings* (2025), <https://doi.org/10.55843/icl2025cong117s>.

¹⁶ Ayan, Op. Cit.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

periodic electoral accountability, did not anticipate and does not straightforwardly constrain. Where such power is exercised without commensurate legal and institutional restraint, the risk is not confined to discrete privacy intrusions but extends to a gradual redistribution of power between citizen and state that is difficult to reverse once the underlying technical infrastructure has been built and normalised within ordinary administrative practice. It is precisely because this risk is structural, cumulative, and only partially visible at the point of initial deployment that the doctrinal and comparative analysis undertaken in this article treats digital surveillance as a central, rather than peripheral, concern of contemporary human rights law.

Two final observations frame the analysis that follows. First, although this article draws primarily on doctrinal and comparative legal scholarship, the underlying phenomenon it examines is fundamentally interdisciplinary: computer science determines what is technically feasible, public administration determines what is institutionally adopted, and law determines what is permissible — and it is only by holding these three dimensions together that a realistic assessment of the human rights implications of smart governance becomes possible. Second, the analysis that follows is deliberately structured to move from description to normative evaluation, rather than beginning with normative critique and searching selectively for supporting examples; this ordering is intended to ensure that the human rights concerns identified are grounded in an accurate account of how smart-governance surveillance actually operates,

rather than in an abstract or hypothetical characterisation of the technology involved.

METHODOLOGY

This article employs a normative (doctrinal) legal research method, which examines law as a coherent system of norms, principles, and rules rather than as an empirical social phenomenon. Three complementary approaches are used in combination. The statutory approach (*pendekatan perundang-undangan*) is applied to examine the relevant legal instruments governing privacy, data protection, and surveillance, including the International Covenant on Civil and Political Rights¹⁷, the European Union's General Data Protection Regulation¹⁸, and Indonesia's Law No. 27 of 2022 on Personal Data Protection¹⁹. The conceptual approach (*pendekatan konseptual*) is used to clarify the meaning and normative content of key doctrinal concepts — including privacy, proportionality, purpose limitation, and algorithmic accountability — as these are developed in contemporary human rights and technology-law scholarship²⁰²¹. The comparative approach (*pendekatan perbandingan*) is used to contrast regulatory responses across jurisdictions, notably the European Union's rights-based regulatory model, Australia's sectoral approach to facial-recognition governance²², and Indonesia's still-maturing data-protection regime, in order to identify transferable lessons and persistent structural weaknesses.

The primary legal materials analysed consist of binding international instruments, regional regulations, and national statutes. The secondary legal materials consist of peer-reviewed journal articles, doctrinal commentaries, and policy analyses published predominantly between 2020 and 2026, sourced through bibliographic databases indexed in Google Scholar and cross-checked

¹⁷ United Nations, International Covenant on Civil and Political Rights (1966), Art. 17.

¹⁸ European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) (2016).

¹⁹ Republik Indonesia, Op. Cit.

²⁰ Okonkwo, Op. Cit. (2023).

²¹ Risse, Op. Cit., p. 351.

²² A Fletcher, "Government Surveillance and Facial Recognition in Australia: A Human Rights Analysis of Recent Developments," *Griffith Law Review* 32, no. 1 (2023): 30, <https://doi.org/10.1080/10383441.2023.2170616>.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

against publisher records (including Taylor & Francis, Elsevier, Oxford University Press, and Internet Policy Review) to verify authorship, publication details, and digital object identifiers. This five-year window was deliberately chosen to capture the most recent doctrinal developments in a field — algorithmic and biometric governance — that has evolved substantially since the COVID-19 pandemic and the proliferation of generative artificial intelligence.

Data collection proceeded through a structured literature search combining the keywords "digital surveillance," "human rights," "smart governance," "smart city," and "data protection," supplemented by citation-tracking of foundational sources to capture doctrinally significant but less frequently indexed contributions. The collected materials were analysed using a qualitative, descriptive-analytical technique: legal norms and scholarly propositions were first mapped according to the human right they most directly implicate (privacy, expression, non-discrimination, or due process), then evaluated against the identified surveillance practices to assess the extent of normative coverage and the presence of enforcement gaps. This technique allows the article to move systematically from description of the surveillance architecture, to identification of the rights at stake, to a reasoned assessment of the adequacy of the corresponding legal safeguards — the analytical sequence that structures the results and discussion presented below.

Two methodological limitations should be acknowledged. First, as a normative legal study, the article does not independently generate empirical data on the technical accuracy, deployment scale, or lived impact of specific surveillance systems; where such empirical findings are referenced, they are drawn from and attributed to the secondary legal and social-science literature reviewed. Second, the comparative dimension of the analysis is necessarily selective rather than exhaustive: the jurisdictions discussed — principally the European Union, Australia, and Indonesia — were selected because the available doctrinal literature allows for a

sufficiently detailed comparison of statutory design and institutional implementation, rather than because they are claimed to be representative of global regulatory practice as a whole. These limitations do not undermine the article's central doctrinal claims but are noted to delineate the appropriate scope of the conclusions drawn.

The methodological choice to combine statutory, conceptual, and comparative approaches, rather than relying on any single approach in isolation, reflects the nature of the subject matter itself. Digital surveillance within smart governance is simultaneously a matter of positive law (what the applicable statutes and treaties actually require), of contested concept (what "privacy," "proportionality," and "algorithmic accountability" mean when applied to technologies their original drafters could not have anticipated), and of comparative institutional design (how different legal systems have translated broadly similar normative commitments into markedly different levels of practical protection). A purely statutory analysis, without the conceptual and comparative dimensions, would risk describing the formal content of the law while missing the substantial gap, documented throughout the results and discussion below, between formal legal text and operational practice.

RESULTS AND DISCUSSION

The Architecture of Smart Governance and the Normalisation of Digital Surveillance

Smart governance, understood as the systematic integration of digital technologies into public administration and urban management, did not emerge as a surveillance project by design. Its origins lie in genuine administrative aspirations: reducing bureaucratic friction, enabling real-time responsiveness to citizens' needs, and improving the evidentiary basis of policymaking. Denmark's digital welfare state, for instance, was conceived primarily as a mechanism to streamline benefit administration and reduce fraud through automated cross-referencing of tax, employment, and residency

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

records²³. Yet the practical effect of this administrative rationalisation has been the construction of comprehensive, continuously updated profiles of individual citizens, profiles that are queried, matched, and scored by algorithms whose decision logic is rarely transparent to the individuals affected.

This pattern recurs across jurisdictions with markedly different political systems. In the smart-city context, closed-circuit television networks equipped with facial-recognition capability, environmental sensors, license-plate readers, and mobility-tracking systems are typically justified by reference to crime prevention, traffic management, and service optimisation. Empirical analysis of smart-city rollouts, however, demonstrates that the deployment of such infrastructure frequently proceeds with limited public consultation and minimal legal safeguards specifically tailored to biometric or locational data, producing what has been described as surveillance "in breach of fundamental human rights" embedded within the very fabric of urban administration²⁴. Command-and-control centres originally designed to coordinate municipal services have, in a number of documented cases, been repurposed as instruments of political and social control, particularly where oversight mechanisms are weak or captured by security agencies²⁵.

Australia offers an instructive illustration of how surveillance infrastructure expands incrementally, often through legislative measures that are individually narrow but cumulatively transformative. Legal analysis of Australia's metadata-retention regime, encryption-decryption powers, and the developing national facial-identification "Capability" shows that each measure was introduced as a discrete, proportionate response to a specific security concern, yet their combined effect is a integrated identification and tracking infrastructure whose compatibility

with international human rights law remains contested even within a mature liberal-democratic legal order²⁶. If such incremental expansion generates serious rights concerns in a jurisdiction with entrenched judicial review and a free press, the risks are considerably more acute in jurisdictions where independent oversight of security and law-enforcement agencies is comparatively underdeveloped²⁷.

A second driver of surveillance normalisation is the blurring of the line between public and private actors in the collection, processing, and monetisation of personal data. Municipal smart-city projects routinely rely on private technology vendors for hardware, cloud storage, and analytics, creating complex public-private data-sharing arrangements that are frequently opaque to affected citizens and, at times, to regulators themselves. Critical scholarship on "consent, coercion, and colonialism" in digital governance argues that this arrangement effectively transfers governmental surveillance capacity to commercial actors whose primary accountability runs to shareholders rather than to citizens, producing a form of data extraction that disproportionately burdens populations with the least capacity to contest it²⁸. This dynamic complicates traditional human rights analysis, which has historically been oriented toward restraining the coercive power of the state, by introducing a set of private intermediaries whose surveillance practices are governed, if at all, by consumer-protection or contract law rather than by human rights obligations directly.

The COVID-19 pandemic served as a significant accelerant of this trend. Digital contact-tracing applications, quarantine-compliance monitoring, and health-status verification systems were deployed at extraordinary speed and scale, frequently on an emergency legal basis that bypassed the ordinary legislative scrutiny applied to

²³ Jørgensen, *Op. Cit.*, p. 123.

²⁴ Alizadeh and Prasad, *Op. Cit.*, p. 1.

²⁵ Ayan, *Op. Cit.*

²⁶ Fletcher, *Op. Cit.*, p. 30.

²⁷ Svobodová, *Op. Cit.*

²⁸ P Moore, P Bloom, and R Nunes, "Consent, Coercion, Colonialism: A Manifesto for Digital Rights from the Left," *Globalizations* 23 (2026): 859, <https://doi.org/10.1080/14747731.2025.2591534>.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

permanent surveillance infrastructure. Assessment of the human rights impact of pandemic-era digital public-health surveillance found that emergency measures, once operational, proved remarkably durable: technical capabilities built for epidemiological purposes were subsequently adapted for border control, law enforcement, and general administrative verification, well beyond their original public-health justification ²⁹. This trajectory exemplifies the phenomenon of "function creep," whereby surveillance systems introduced for a narrowly defined, ostensibly legitimate purpose are progressively repurposed for objectives that were never subject to the proportionality assessment applied — however imperfectly — to the original deployment.

A further structural feature of the smart-governance surveillance architecture is its reliance on predictive and profiling analytics rather than retrospective investigation alone. Where traditional surveillance was oriented toward the collection of evidence concerning a specific, already-suspected individual, contemporary systems increasingly generate risk scores, behavioural predictions, and anomaly flags across entire populations, identifying individuals for further scrutiny on the basis of patterns detected within aggregated data. Comparative legal analysis of artificial-intelligence-enabled surveillance across democratic and authoritarian regimes alike shows that predictive policing and social-monitoring systems are deployed to suppress dissent and monitor political opposition to varying degrees in both types of political system, differing chiefly in the intensity and transparency of their application rather than in their underlying technical logic ³⁰³¹. This

convergence complicates the assumption, common in earlier surveillance scholarship, that robust democratic institutions alone are sufficient to prevent surveillance overreach; institutional design and enforceable legal constraint, rather than regime type as such, appear to be the decisive variables ³².

Digital identity systems constitute a further, distinct layer of this architecture, one that is frequently treated in policy discourse as a purely administrative convenience rather than a surveillance-relevant technology. Centralised biometric identity databases — linking fingerprints, facial templates, or iris scans to a single national identifier used across tax, banking, health, and welfare systems — are increasingly presented as prerequisites for "smart" public-service delivery. Once such a unified identifier exists, however, it becomes technically trivial to aggregate an individual's interactions across otherwise unrelated public and private systems, producing a comprehensiveness of state knowledge that has no clear historical precedent outside of authoritarian population-control regimes. Doctrinal commentary on citizenship in the digital age observes that the rights and responsibilities historically associated with citizenship are being quietly redefined by the technical architecture of digital identity systems, such that access to an ordinary public service can become conditional upon acceptance of biometric enrolment, with limited practical opportunity for individuals to decline ³³. Where digital identity infrastructure is layered onto pre-existing weaknesses in institutional oversight, the resulting system combines the efficiency benefits of unified identification with a surveillance capacity that significantly exceeds what any single sectoral

²⁹ Sekalala et al., *Op. Cit.*, p. 7.

³⁰ H W H Chan and N Lo, "A Study on Human Rights Impact with the Advancement of Artificial Intelligence," *Journal of Posthumanism* (2025), <https://doi.org/10.63332/joph.v5i2.490>.

³¹ V K Katiyar and S Singh, "Human Rights Challenges in the Contemporary World: Re-Examining Law and Technology in the Digital Era," *EPRA International Journal of Multidisciplinary*

Research (IJMR) (2026), <https://doi.org/10.36713/epra26963>.

³² R P Kunjukrishnan and S Krishnakumariam, "Artificial Intelligence and Human Rights in the Era of Digital Governance: Exploring Promises and Challenges," *International Journal of Advances in Social Sciences and Humanities* (2025), <https://doi.org/10.56225/ijassh.v4i2.401>.

³³ Georgekutty, *Op. Cit.*

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

agency would have been authorised to build independently.

The accountability of private technology vendors constitutes a related structural gap. Because much of the hardware, software, and analytical capability underlying smart-governance surveillance is procured from commercial suppliers, the effective governance of these systems depends heavily on the terms of public procurement contracts — instruments that are rarely drafted with human rights compliance as a primary design consideration and rarely subject to the same standard of judicial or parliamentary scrutiny as primary legislation. Comparative analysis of AI-enabled surveillance procurement notes that vendors frequently retain proprietary control over the underlying algorithms, such that neither the procuring government agency nor affected citizens can fully audit the logic by which identification, scoring, or risk-flagging decisions are produced³⁴. This opacity is compounded where a small number of multinational vendors supply comparable surveillance technology across many jurisdictions simultaneously, creating a *de facto* standardisation of surveillance capability that outpaces the comparatively fragmented, jurisdiction-specific development of corresponding legal safeguards³⁵.

The predictive dimension of this architecture deserves further elaboration, since it represents the point at which smart governance departs most sharply from earlier models of state surveillance. Predictive-policing and social-risk-scoring systems operate by training statistical models on historical administrative and criminal-justice data, and then applying the resulting model to flag individuals, addresses, or neighbourhoods for heightened scrutiny. Because the historical data on which such models are trained typically reflects prior patterns of policing intensity — patterns that are themselves frequently uneven across ethnic, religious, or socio-economic

lines — the resulting predictions tend to reproduce and, in some documented instances, to amplify pre-existing enforcement disparities, even where the system's designers had no discriminatory intent³⁶. Doctrinal literature on human rights and technology characterises this feedback loop as one of the central accountability challenges of algorithmic governance: the harm is generated not by a single identifiable decision-maker exercising discretion, but by the cumulative interaction of historical data, statistical modelling choices, and downstream administrative action, a structure that existing anti-discrimination and administrative-law doctrine — built around individualised decision review — was not designed to address³⁷.

The geographic distribution of smart-governance surveillance capacity further complicates the human rights analysis. Empirical accounts of smart-city rollouts in the global South emphasise that municipal authorities in resource-constrained settings frequently adopt turnkey surveillance packages offered by external vendors on preferential financing terms, a practice that accelerates technological adoption but simultaneously reduces the domestic bargaining power available to negotiate rights-protective contractual terms, technical standards, or data-localisation requirements³⁸. The consequence is a form of asymmetric technological dependency in which the pace of surveillance-capability adoption significantly outstrips the pace of corresponding domestic legal and institutional capacity-building — a dynamic that is directly relevant to Indonesia's own experience of rapid smart-city expansion alongside a still-maturing data-protection institutional framework³⁹.

Taken together, these developments demonstrate that the surveillance embedded within smart governance is neither incidental nor easily reversible. It is structurally generated by the administrative logic of data-driven

³⁴ Chan and Lo, Op. Cit.

³⁵ Moore, Bloom, and Nunes, Op. Cit., p. 859.

³⁶ Chan and Lo, Op. Cit.

³⁷ Land and Aronson, Op. Cit.

³⁸ Moore, Bloom, and Nunes, Op. Cit., p. 859.

³⁹ Ananda and Ikraam, Op. Cit.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

governance itself: efficiency gains are achieved precisely because systems collect, retain, and cross-reference personal data at a scale and granularity that would have been technically or economically infeasible under earlier administrative models. The following sub-section turns from this descriptive account of the surveillance architecture to an analysis of the specific human rights it places at risk, and of the extent to which existing legal frameworks are equipped to respond.

It is also necessary to situate this architecture within a longer intellectual history of surveillance theory, since much of the anxiety surrounding smart governance echoes concerns articulated long before the advent of artificial intelligence or the Internet of Things. Classical accounts of disciplinary power emphasised that the mere possibility of being observed, rather than continuous observation itself, is sufficient to alter behaviour — a dynamic that smart-governance infrastructure reproduces at a societal scale previously unattainable. What distinguishes the contemporary situation from earlier surveillance regimes is not the underlying disciplinary logic, which is well theorised, but the technical capacity to operationalise that logic continuously, automatically, and across an entire population simultaneously, without the resource constraints that historically limited the reach of state observation to a comparatively small number of specifically targeted individuals. Contemporary human rights scholarship on artificial intelligence and governance frames this shift as a change not merely of degree but of kind, since population-scale, continuously updated profiling alters the very conditions under which individual autonomy and political participation are exercised⁴⁰.

The applicability of human rights obligations to the private technology vendors that supply much of this infrastructure remains one of the more doctrinally unsettled dimensions of the field. International human

rights law was developed principally to constrain state conduct, and while emerging business-and-human-rights frameworks extend certain due-diligence expectations to private actors, these expectations are typically framed as voluntary or reputational commitments rather than binding legal obligations enforceable through the same mechanisms that apply to state conduct⁴¹. Where a private vendor designs, builds, and operates a facial-recognition or predictive-analytics system on behalf of a government client, responsibility for any resulting rights violation is frequently contested between the procuring public authority and the supplying private vendor, a jurisdictional and doctrinal ambiguity that surveillance-oriented literature identifies as a significant practical obstacle to effective accountability, particularly in jurisdictions where public procurement law does not expressly extend human rights due-diligence obligations to technology suppliers⁴².

Finally, it is important to note that the architecture described in this sub-section is not static; it is continuously extended by successive waves of technical innovation, most recently the integration of generative artificial-intelligence systems into administrative decision-support tools. Where earlier surveillance infrastructure was primarily oriented toward the collection and matching of discrete data points — a location, a transaction, a biometric template — contemporary systems increasingly generate synthetic inferences: probabilistic assessments of an individual's future conduct, risk profile, or eligibility status derived from patterns that no single human reviewer specified in advance. This shift from data collection to inference generation represents the frontier of the surveillance architecture examined in this article, and it is precisely this frontier — rather than the comparatively well-studied practice of CCTV or metadata retention — that existing legal frameworks are least well equipped to address, since the harm in question arises not from the

⁴⁰ Kunjukrishnan and Krishnakumariam, Op. Cit.

⁴¹ Land and Aronson, Op. Cit.

⁴² Moore, Bloom, and Nunes, Op. Cit., p. 859.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

disclosure of a fact the individual sought to keep private, but from the generation of a new, potentially inaccurate or unfair characterisation of the individual that did not exist in any single dataset prior to algorithmic processing⁴³⁴⁴.

B. Human Rights at Risk: Privacy, Expression, Equality, and the Adequacy of Legal Safeguards

The right most directly implicated by digital surveillance is the right to privacy, protected under Article 17 of the International Covenant on Civil and Political Rights, which prohibits arbitrary or unlawful interference with an individual's privacy, family, home, or correspondence⁴⁵. International human rights bodies have long interpreted this provision to require that any interference be provided for by law, pursue a legitimate aim, and be necessary and proportionate to that aim. Contemporary surveillance practice tests each element of this standard. The "law" authorising data collection is frequently drafted in broad, technology-neutral terms that were never designed to anticipate biometric identification or predictive analytics; the "legitimate aim" invoked — usually public security or administrative efficiency — is rarely accompanied by a demonstrated evidentiary link between the surveillance measure and the stated objective; and "necessity and proportionality" assessments, where they exist at all, are typically conducted internally by the implementing agency rather than by an independent body with the authority to refuse or modify the measure⁴⁶⁴⁷.

Regional and national data-protection frameworks were designed, in part, to operationalise this proportionality standard for the digital context. The European Union's General Data Protection Regulation establishes

purpose limitation, data minimisation, and accountability as binding legal principles, backed by an independent supervisory authority with meaningful enforcement powers, including substantial financial penalties⁴⁸. Indonesia's Law No. 27 of 2022 adopts a broadly comparable structure, recognising personal data protection as an extension of the constitutional right to privacy and imposing obligations of lawful basis, purpose limitation, and data-subject consent on data controllers⁴⁹. Doctrinal assessment of the PDP Law's early implementation, however, identifies significant gaps: the personal-data supervisory authority mandated by the statute had not, at the time of the most recent scholarly review, been established as a fully independent institution; sector-specific implementing regulations remain incomplete; and the law's application to data processing conducted by state agencies for security or administrative purposes remains doctrinally unsettled⁵⁰. These gaps are consequential precisely because it is state, rather than purely commercial, data processing that carries the greatest capacity to translate privacy interference into concrete restrictions on liberty.

A second right placed at risk is freedom of expression, operating principally through the mechanism of the "chilling effect." Empirical and doctrinal literature converges on the finding that individuals who are aware, or reasonably suspect, that their communications or movements are subject to surveillance tend to self-censor political speech, avoid association with disfavoured groups, and curtail participation in public protest, independent of whether the surveillance measure is ever formally invoked against them⁵¹. Risse's account of epistemic rights extends this concern

⁴³ Okonkwo, Op. Cit. (2023).

⁴⁴ O A Okonkwo, "Evolving Interpretations of Digital Privacy, Free Expression, and Data Protection within International Human Rights Jurisprudence and Governance Frameworks," International Journal of Science and Research Archive (2025), <https://doi.org/10.30574/ijrsra.2025.17.1.2876>.

⁴⁵ United Nations, Op. Cit., Art. 17.

⁴⁶ Sethi, Ullah, and Naseem, Op. Cit.

⁴⁷ D Nandy, "Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns," Journal of Current Social and Political Issues (2023), <https://doi.org/10.15575/jcspi.v1i1.442>.

⁴⁸ European Union, Op. Cit.

⁴⁹ Republik Indonesia, Op. Cit.

⁵⁰ Muzairoh, Noviasari, and Syafingi, Op. Cit.

⁵¹ Talapina, Op. Cit.

further, arguing that pervasive algorithmic profiling threatens not merely the expression of existing views but the individual's capacity to form and revise beliefs autonomously, since profiling systems increasingly curate the informational environment within which political and social reasoning takes place ⁵². Katiyar and Singh similarly emphasise that the digital era requires a re-examination of established human rights doctrine, since classical civil-liberties frameworks were not designed to address harms that are diffuse, cumulative, and largely invisible to the individuals affected ⁵³.

Non-discrimination and equality before the law constitute a third area of significant risk, arising principally from the deployment of biometric identification and predictive-analytics systems whose algorithmic accuracy varies systematically across demographic groups. Facial-recognition systems, in particular, have been repeatedly documented to exhibit materially higher error rates for women and for individuals with darker skin tones, a technical disparity that translates directly into unequal exposure to misidentification, wrongful investigative scrutiny, and, in policing contexts, wrongful detention ⁵⁴. Analysis of smart-city deployments in both the global North and the global South confirms that these disparities are not merely theoretical but recur across jurisdictions with markedly different technological infrastructure, suggesting a structural rather than incidental flaw in the current generation of biometric surveillance tools ⁵⁵. Some jurisdictions have begun to respond through transparency-oriented governance innovations; a Brazilian initiative to build a "human rights smart city" transparency-identification system, for example, seeks to make the operation of municipal surveillance and identification

systems auditable by affected communities, illustrating that technical and institutional design choices can meaningfully mitigate, though not eliminate, discriminatory risk ⁵⁶.

Due process and accountability form a fourth, closely related dimension of concern. Where individuals are subject to algorithmically generated risk scores, automated eligibility determinations, or predictive-policing flags, the practical capacity to know the basis of an adverse decision, let alone to contest it before an independent body, is frequently absent. Scholarship on the evolving interpretation of digital privacy and data protection within international human rights jurisprudence emphasises that meaningful due process in the algorithmic context requires, at minimum, a right to explanation, a right to meaningful human review, and an accessible mechanism for redress — elements that remain unevenly codified across both international soft-law instruments and domestic legislation ⁵⁷. The cybersecurity dimension of this problem compounds the difficulty: because surveillance and identification systems are simultaneously targets of malicious cyberattack and instruments of potential state overreach, effective governance must reconcile security-hardening measures with transparency and accountability obligations that are, in institutional practice, frequently treated as competing rather than complementary objectives ⁵⁸.

The governance-design literature identifies notice-and-choice mechanisms — the individual consent frameworks historically central to data-protection law — as increasingly inadequate to this environment. Analysis of surveillance and privacy as "coevolving disruptions" demonstrates that as governmental and commercial data-collection capabilities

⁵² Risse, *Op. Cit.*, p. 351.

⁵³ Katiyar and Singh, *Op. Cit.*

⁵⁴ Fletcher, *Op. Cit.*, p. 30.

⁵⁵ Alizadeh and Prasad, *Op. Cit.*, p. 1.

⁵⁶ R Souza et al., "My Human Rights Smart City: Improving Human Rights Transparency Identification System," *Sustainability* (2024), <https://doi.org/10.3390/su16031274>.

⁵⁷ Okonkwo, *Op. Cit.* (2025).

⁵⁸ R Shawe, "Cybersecurity and Human Rights: Navigating the Balance between Security and Freedom in the Digital Era," *Journal of Information Technology and Integrity* (2025), <https://doi.org/10.33790/jiti1100110>.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

have expanded, the practical meaningfulness of individual consent has correspondingly diminished: citizens interacting with smart-city infrastructure, unlike users of a discrete digital service, typically cannot decline to be observed by public-space sensors or municipal identification systems without forgoing access to essential services altogether⁵⁹. This structural asymmetry suggests that legal frameworks premised primarily on individual consent are poorly matched to an infrastructure of ambient, continuous, largely non-optional data collection, and that rights protection in this domain must instead be secured through ex ante regulatory constraint — purpose limitation, necessity and proportionality review, and independent oversight — rather than through the fiction of informed individual choice⁶⁰.

Comparative analysis of regulatory responses reinforces this conclusion. Jurisdictions that have paired data-protection legislation with an independent, adequately resourced supervisory authority and a codified proportionality standard for security-related data processing demonstrate materially stronger rights protection than those relying on data-protection statutes alone, however comprehensive those statutes may appear on their face⁶¹. Indonesia's continuing effort to operationalise the PDP Law's institutional framework, alongside its parallel smart-city and electronic-government initiatives, occupies an instructive intermediate position: the statutory architecture increasingly resembles international best practice, yet institutional capacity, sectoral implementing regulation, and — critically — the scope of the law's application to state security agencies remain unresolved questions with direct human rights consequences^{62,63}. Addressing these gaps is not a matter of drafting additional legal text alone; it requires embedding human-rights-based design principles directly into the technical

architecture of smart-governance systems, together with institutional mechanisms — independent supervisory authorities, mandatory human rights impact assessments prior to deployment, and accessible redress procedures — capable of translating legal principle into enforceable practice^{64,65}.

The intersection of surveillance harms with existing patterns of social and economic inequality deserves explicit treatment, since the human rights impact of smart governance is rarely distributed evenly across a population. Individuals who depend most heavily on state-administered welfare, housing, or health services — typically among the poorest members of society — are also those whose data is most extensively collected, cross-referenced, and algorithmically assessed, since eligibility determination for such services increasingly relies on automated verification against multiple government databases. By contrast, individuals with greater financial means, who rely less on directly state-administered services and more on private-sector alternatives, are correspondingly less exposed to this particular form of state data processing, even though they may be subject to comparable commercial surveillance through consumer technology. Doctrinal analysis of the digital welfare state captures this asymmetry precisely: automated fraud-detection and eligibility systems, however neutrally designed in principle, in practice concentrate their investigative and verificatory attention on precisely the population least equipped, in terms of time, legal knowledge, and financial resources, to contest an erroneous algorithmic determination⁶⁶. A human-rights-based evaluation of smart governance must therefore attend not only to the formal content of the applicable legal safeguards but to the differential practical burden those safeguards

⁵⁹ A B Whitford and J Yates, "Surveillance and Privacy as Coevolving Disruptions: Reflections on "Notice and Choice"," Policy Design and Practice 6, no. 1 (2022): 14, <https://doi.org/10.1080/25741292.2022.2086667>.

⁶⁰ Georgekutty, Op. Cit.

⁶¹ Wernick and Artyushina, Op. Cit.

⁶² Ananda and Ikraam, Op. Cit.

⁶³ Muzairoh, Noviasari, and Syafingi, Op. Cit.

⁶⁴ Kunjukrishnan and Krishnakumariam, Op. Cit.

⁶⁵ Nandy, Op. Cit.

⁶⁶ Jørgensen, Op. Cit., p. 123.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

place on different segments of the population they are meant to protect.

Particular attention is warranted for the position of children and other groups whose vulnerability to surveillance-related harm is heightened rather than mitigated by claims of protective purpose. Digital age-verification systems, biometric school-attendance monitoring, and child-safety-oriented content-moderation infrastructure are frequently justified by reference to child protection, yet the same technical architecture that enables the identification of a minor for protective purposes also enables their identification, tracking, and profiling for purposes entirely unrelated to child welfare, with limited independent evaluation of whether the protective benefit in fact outweighs the surveillance cost imposed on the broader population subject to the same system ⁶⁷. Human rights doctrine addressing the digital era increasingly recognises that protective justifications, precisely because they carry strong intuitive legitimacy, require heightened rather than relaxed scrutiny of the proportionality and necessity of the resulting surveillance measure ⁶⁸.

A further comparative dimension concerns the emerging generation of artificial-intelligence-specific regulation, exemplified by the European Union's risk-tiered approach to AI governance, which classifies biometric identification and law-enforcement profiling systems as inherently "high-risk" and subjects them to mandatory conformity assessment, human oversight requirements, and registration obligations prior to deployment. This risk-tiered model offers a potentially transferable template for jurisdictions such as Indonesia, whose existing legal architecture — comprising the PDP Law, sectoral electronic-government regulations, and general administrative law — currently lacks an equivalent instrument specifically calibrated to the distinctive risks of biometric and predictive-analytics systems

deployed within public administration ⁶⁹⁷⁰. Absent such an instrument, the burden of ensuring proportionate deployment falls disproportionately on the general, necessarily more abstract standards of constitutional and international human rights law, standards that — as the preceding analysis has shown — are considerably more difficult to enforce against a specific, already-operational surveillance system than a purpose-built *ex ante* authorisation requirement would be ⁷¹.

Finally, the adequacy of legal safeguards cannot be assessed in the abstract; it must be evaluated against the realistic capacity of affected individuals to invoke them. Formal rights of access, correction, and objection under data-protection statutes are of limited practical value where the individuals most exposed to smart-governance surveillance — often lower-income, rural, or otherwise marginalised populations who depend most heavily on digitalised public services — lack the legal literacy, resources, or institutional access necessary to exercise those rights meaningfully ⁷². Closing this implementation gap requires not only stronger statutory text but sustained investment in independent legal-aid capacity, public legal education concerning data rights, and supervisory authorities empowered to initiate proactive, rather than purely complaint-driven, investigation of high-risk smart-governance deployments ⁷³.

The right to an effective remedy, guaranteed under general international human rights law as a corollary to the substantive rights discussed above, warrants separate emphasis because it functions as the procedural mechanism through which every other right examined in this article is, in practice, enforced or left unenforced. An effective remedy in the surveillance context requires, at minimum, that the individual be able to learn that a surveillance measure has been applied to them, that they have access to an independent body

⁶⁷ Ayan, Op. Cit.

⁶⁸ Kunjukrishnan and Krishnakumariamamma, Op. Cit.

⁶⁹ Okonkwo, Op. Cit. (2025).

⁷⁰ Wernick and Artyushina, Op. Cit.

⁷¹ Land and Aronson, Op. Cit.

⁷² Sethi, Ullah, and Naseem, Op. Cit.

⁷³ Muzairoh, Noviasari, and Syafingi, Op. Cit.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

competent to assess the lawfulness of that measure, and that the body in question has the practical authority to order cessation of unlawful processing, deletion of unlawfully obtained data, and, where appropriate, compensation. Comparative doctrinal analysis of contemporary human rights challenges in the digital era finds that each element of this remedial chain is commonly deficient in practice: notification requirements are frequently subject to broad national-security exceptions that leave affected individuals permanently unaware that a measure was applied to them; independent review bodies, where they exist, often lack the technical expertise necessary to meaningfully assess algorithmic decision-making; and remedial powers, even where formally available, are rarely exercised against public authorities with the same rigour applied to private-sector data controllers⁷⁴⁷⁵.

A growing body of scholarship frames the cumulative response to these deficiencies as an emerging project of "digital constitutionalism": the effort to articulate, through a combination of hard law, judicial interpretation, and institutional design, a set of constitutional-grade constraints specifically adapted to the exercise of algorithmic and data-driven public power, in the same way that earlier constitutional traditions developed specific constraints on policing, taxation, and administrative discretion⁷⁶. Whether this project ultimately produces binding, universally applicable standards, or instead remains a fragmented patchwork of regional and sectoral instruments, will substantially determine whether the tension identified throughout this article — between the efficiency promise of smart governance and the human rights obligations that bind the states deploying it — is resolved through deliberate legal design or is instead allowed to resolve itself, by default, in favour of expanding surveillance capacity⁷⁷.

Judicial and quasi-judicial review of surveillance measures offers a further lens through which to assess the adequacy of existing safeguards. Where courts have engaged directly with digital surveillance measures, the resulting jurisprudence has generally affirmed the applicability of established necessity and proportionality doctrine to novel biometric and data-driven contexts, while stopping short of establishing categorical prohibitions on any particular surveillance technology. Comparative analysis of judicial engagement with government surveillance and facial-recognition programmes shows courts applying long-standing proportionality tests to distinctly new factual circumstances, an approach that provides doctrinal continuity but also means that the practical protection afforded to individuals depends heavily on the quality and specificity of the evidentiary record placed before the reviewing court by litigants and, ultimately, on the accessibility of judicial review as a remedy in the first place⁷⁸. In jurisdictions where constitutional or administrative litigation is costly, slow, or otherwise inaccessible to the individuals most exposed to smart-governance surveillance, the formal availability of judicial review provides comparatively little practical protection, reinforcing the article's broader argument that *ex ante* regulatory constraint, rather than reliance on litigation after the fact, should be treated as the primary safeguard⁷⁹.

International soft-law and policy guidance has, in recent years, begun to converge on a broadly consistent set of principles for the human-rights-compliant governance of surveillance technologies: legality, necessity, proportionality, non-discrimination, transparency, and the availability of an effective remedy. The persistent difficulty, evident throughout the literature reviewed for this article, lies not in articulating these principles — on which there is now substantial doctrinal consensus — but in

⁷⁴ Katiyar and Singh, Op. Cit.

⁷⁵ Ayan, Op. Cit.

⁷⁶ Chan and Lo, Op. Cit.

⁷⁷ Svobodová, Op. Cit.

⁷⁸ Fletcher, Op. Cit., p. 30.

⁷⁹ Nandy, Op. Cit.

P-ISSN
E-ISSN
DOI
Available

: 0000-0000
: 3031-6782
: <https://doi.org/10.61942/jhk.v3i5.667>
: <https://jurnalhafasy.com/index.php/jhk>

Vol. 3 No. 5, August 2026

translating them into binding, sector-specific, and technically operational legal requirements capable of guiding the day-to-day procurement and design decisions of public administrators long before any court or supervisory authority is called upon to review the resulting system⁸⁰⁸¹. It is this translation gap, between widely accepted principle and technically operational legal rule, that the recommendations set out in the concluding section seek most directly to address.

Comparative regulatory experience nonetheless offers grounds for cautious optimism. The trajectory of European data-protection law demonstrates that a legal framework initially perceived as unduly burdensome by regulated industries can, over time, become normalised as a baseline expectation of responsible data governance, shaping procurement standards and technical design practice well beyond the jurisdiction in which the framework was originally enacted. Indonesia's PDP Law, though younger and less institutionally mature than its European counterpart, was drafted with evident awareness of this comparative experience, and its core structural principles — lawful basis, purpose limitation, data-subject rights, and independent supervision — align closely with international best practice on their face⁸²⁸³. The central task facing Indonesian policymakers, legal practitioners, and civil society is therefore less one of fundamental statutory redesign than of sustained institutional implementation: fully establishing the independent supervisory authority the law contemplates, issuing the sectoral implementing regulations necessary to give the statute operational precision in the context of public-sector surveillance specifically, and building the administrative and judicial capacity necessary to enforce the law's guarantees in practice rather than merely on the page⁸⁴.

CONCLUSION

This article has examined the structural tension between the administrative promise of smart governance and the human rights obligations that international and domestic law impose upon states deploying digital surveillance technologies. The analysis shows that the surveillance architecture underlying contemporary smart governance — biometric identification, networked sensor infrastructure, predictive analytics, and expansive public-private data-sharing arrangements — is not an incidental by-product of technological modernisation but a structural feature of the administrative logic that makes such governance "smart" in the first place. This architecture places at risk a cluster of interrelated human rights: privacy and data protection under Article 17 of the International Covenant on Civil and Political Rights; freedom of expression, through the well-documented chilling effect of pervasive monitoring and, more fundamentally, through threats to epistemic autonomy; equality before the law, through demonstrated demographic disparities in biometric identification accuracy; and due process, through the frequent absence of meaningful explanation, human review, and accessible redress for algorithmically generated decisions. Existing legal frameworks, both international and domestic, provide an important but presently insufficient foundation for addressing these risks. The International Covenant on Civil and Political Rights establishes the applicable normative standard of legality, necessity, and proportionality, but its general formulation offers limited operational guidance for algorithmic and biometric surveillance specifically. Regional instruments such as the European Union's General Data Protection Regulation demonstrate that a more operationally precise, independently enforced framework is achievable, while Indonesia's Law No. 27 of 2022 represents meaningful domestic progress that nonetheless remains constrained by incomplete institutional implementation, particularly regarding

⁸⁰ Shawe, Op. Cit.

⁸¹ Okonkwo, Op. Cit. (2023).

⁸² Republik Indonesia, Op. Cit.

⁸³ European Union, Op. Cit.

⁸⁴ Muzairoh, Noviasari, and Syafingi, Op. Cit.

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
 E-ISSN : 3031-6782
 DOI : <https://doi.org/10.61942/jhk.v3i5.667>
 Available : <https://jurnalhafasy.com/index.php/jhk>

independent supervisory capacity and the law's application to state security-related data processing.

REFERENCE

- Alizadeh, T., & Prasad, D. (2026). Smart city initiatives, practices and technologies: surveillance in breach of fundamental human rights. *Telematics and Informatics*, 106, 102391. <https://doi.org/10.1016/j.tele.2026.102391>
- Ananda, M., & Ikraam, A. (2026). Perlindungan Hak Asasi Manusia Pada Era Pengawasan Digital Oleh Negara: Analisis Hukum Tentang Privasi Vs Keamanan. *Jurnal Locus Penelitian dan Pengabdian*. <https://doi.org/10.58344/locus.v5i1.5459>
- Ayan, J. (2026). The Effect of Digital Surveillance Systems and Their Implications for Civil Liberties in Smart Societies. *Bolan International Journal of Research Insights (BIJRI)*. <https://doi.org/10.66021/bijri.v3i1.41>
- Chan, H. W. H., & Lo, N. (2025). A Study on Human Rights Impact with the Advancement of Artificial Intelligence. *Journal of Posthumanism*. <https://doi.org/10.63332/joph.v5i2.490>
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
- Fletcher, A. (2023). Government surveillance and facial recognition in Australia: a human rights analysis of recent developments. *Griffith Law Review*, 32(1), 30–61. <https://doi.org/10.1080/10383441.2023.2170616>
- Georgekutty, D. (2025). Citizenship in the Digital Age: Rights, Responsibilities, and Surveillance. *International Journal of Social Science Research Studies (IJSSRS)*. <https://doi.org/10.63090/ijssrs/3108.1932.0005>
- Jørgensen, R. (2021). Data and rights in the digital welfare state: the case of Denmark. *Information, Communication & Society*, 26, 123–138. <https://doi.org/10.1080/1369118x.2021.1934069>
- Katiyar, V. K., & Singh, S. (2026). Human Rights Challenges in the Contemporary World: Re-examining Law and Technology in the Digital Era. *EPRA International Journal of Multidisciplinary Research (IJMR)*. <https://doi.org/10.36713/epra26963>
- Kunjukrishnan, R. P., & Krishnakumariamamma, S. (2025). Artificial Intelligence and Human Rights in the Era of Digital Governance: Exploring Promises and Challenges. *International Journal of Advances in Social Sciences and Humanities*. <https://doi.org/10.56225/ijassh.v4i2.401>
- Land, M., & Aronson, J. (2020). Human Rights and Technology: New Challenges for Justice and Accountability. *Annual Review of Law and Social Science*. <https://doi.org/10.1146/annurev-lawsocsci-060220-081955>
- Moore, P., Bloom, P., & Nunes, R. (2026). Consent, coercion, colonialism: a manifesto for digital rights from the left. *Globalizations*, 23, 859–878. <https://doi.org/10.1080/14747731.2025.2591534>
- Muzairroh, E., Noviasari, D. T., & Syafingi, H. M. (2024). Analisis Perlindungan Hukum Terhadap Privasi Data Pribadi di Era Digital dalam Prespektif Hak Asasi Manusia. *Borobudur Law and Society Journal*, 3(1), 31–36. <https://doi.org/10.31603/11824>
- Nandy, D. (2023). Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns. *Journal of Current Social and Political Issues*. <https://doi.org/10.15575/jespi.v1i1.442>
- Okonkwo, O. A. (2023). Ethical tensions between AI surveillance architectures, human rights preservation, and the universal entitlement to digital privacy and dignity. *Magna Scientia Advanced*

P-ISSN : 0000-0000 Vol. 3 No. 5, August 2026
 E-ISSN : 3031-6782
 DOI : <https://doi.org/10.61942/jhk.v3i5.667>
 Available : <https://jurnalhafasy.com/index.php/jhk>

- Research and Reviews, 9(2).
<https://doi.org/10.30574/msarr.2023.9.2.0179>
- Okonkwo, O. A. (2025). Evolving interpretations of digital privacy, free expression, and data protection within international human rights jurisprudence and governance frameworks. *International Journal of Science and Research Archive*.
<https://doi.org/10.30574/ijrsra.2025.17.1.2876>
- Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Risse, M. (2021). The Fourth Generation of Human Rights: Epistemic Rights in Digital Lifeworlds. *Moral Philosophy and Politics*, 8, 351–378.
<https://doi.org/10.1515/mopp-2020-0039>
- Sekalala, S., Dagron, S., Forman, L., & Meier, B. (2020). Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights*, 22(2), 7–20.
<https://doi.org/10.17615/8e8a-m957>
- Sethi, A., Ullah, H. H., & Naseem, R. M. S. (2025). Surveillance, National Security and the Right to Privacy in the Digital Era. *The Critical Review of Social Sciences Studies*.
<https://doi.org/10.59075/gf564d60>
- Shawe, R. (2025). Cybersecurity and Human Rights: Navigating the Balance between Security and Freedom in the Digital Era. *Journal of Information Technology and Integrity*.
<https://doi.org/10.33790/jiti1100110>
- Souza, R., Cezario, B., Affonso, E., Machado, A., Vieira, D., Chinelli, C., Haddad, A., Dusek, P., Miranda, M., Soares, C., & Guedes, A. (2024). My Human Rights Smart City: Improving Human Rights Transparency Identification System. Sustainability.
<https://doi.org/10.3390/su16031274>
- Svobodová, T. (2025). Recalibrating Liberty and Security: Human Rights Challenges in the Age of Mass Surveillance. *Congress Proceedings*.
<https://doi.org/10.55843/icl2025cong117s>
- Talapina, E. (2021). Surveillance and human rights: new risks in the digital age. *Sravnitel'noe konstitucionnoe obozrenie*.
<https://doi.org/10.21128/1812-7126-2021-6-123-136>
- United Nations. (1966). *International Covenant on Civil and Political Rights*.
- Wernick, A., & Artyushina, A. (2023). Future-proofing the city: A human rights-based approach to governing algorithmic, biometric and smart city technologies. *Internet Policy Review*, 12(1).
<https://doi.org/10.14763/2023.1.1695>
- Whitford, A. B., & Yates, J. (2022). Surveillance and privacy as coevolving disruptions: reflections on "notice and choice". *Policy Design and Practice*, 6(1), 14–26.
<https://doi.org/10.1080/25741292.2022.2086667>