Otoritas : Jurnal Ilmu Pemerintahan Vol. 15, No. 3, 2025
DOI: https://doi.org/10.26618/ojip.v15i3.19703

Artificial intelligence surveillance and the right to privacy in Vietnam a human security policy

Nguyen Nam Trung[*)]
Faculty of Law, Ho Chi Minh City University of Economics and Finance, Vietnam

Abstract

The rapid expansion of artificial intelligence (AI)–enabled surveillance has become a central feature of contemporary governance, enhancing public security while raising serious concerns for the right to privacy. This article examines AI surveillance in Vietnam through the combined lenses of human security and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Using doctrinal legal analysis and focused comparative evaluation, the study analyses how AI surveillance practices—such as facial recognition, biometric profiling, and behavioural analytics—generate cumulative privacy risks, including informational opacity, behavioural chilling, algorithmic bias, and institutional accountability deficits. It further assesses whether Vietnam's existing legal framework, particularly the Law on Cybersecurity and Decree 13/2023/NĐ-CP, satisfies ICCPR standards of legality, legitimate aim, necessity, proportionality, and effective oversight. The findings reveal significant normative and institutional gaps. Drawing on comparative insights from the EU's GDPR and South Korea's PIPA, the article proposes a phased and context-sensitive reform pathway to strengthen privacy protection while supporting Vietnam's digital transformation and national-security objectives.

Keywords: *artificial intelligence surveillance, right to privacy, human security*

*)corresponding author
Email: trungnn@uef.edu.vn

Introduction

The rapid and widespread development of artificial intelligence (AI) has become a defining feature of contemporary governance (Ghosh et al., 2025; Taeihagh, 2021). AI technologies now support national-security operations, public-order management, and emergency response systems across many jurisdictions (Haney, 2019; National Security Commission on Artificial Intelligence, 2021; Reddy et al., 2024; Sakpal, 2024). In particular, AI-enabled surveillance tools, such as facial-recognition systems, automated number-plate readers, predictive algorithms, and behaviour-detection cameras, are widely used to increase monitoring capacity and operational efficiency. These systems enhance the ability to detect traffic violations, monitor large crowds in real time, identify suspects more rapidly, and respond more effectively to emerging threats. For many governments, integrating AI into surveillance infrastructures has therefore become both technologically inevitable and strategically essential.

Nonetheless, the expansion of AI-driven surveillance raises significant risks for the right to privacy (Ergashev, 2023; Johari & Sparviero, 2025; Singh, 2024). When examined through the lens of human security, privacy functions not only as a legal entitlement but as a safeguard for personal dignity, autonomy, and freedom from undue intrusion (UNDP, 1994). Unregulated or poorly governed AI surveillance may

result in continuous tracking of individuals, opaque data processing, profiling without consent, and heightened risks of data misuse or leakage. Global surveys indicate that a majority of respondents fear AI-based monitoring technologies may be used beyond their stated purposes, particularly when implemented without clear transparency or independent oversight (Ezzeddine et al., 2023) These concerns illustrate the growing tension between the pursuit of national security and the protection of human security, whereby efforts to strengthen state capacity can inadvertently erode privacy and public trust (Zuboff, 2023). Understanding these risks is essential for evaluating whether AI surveillance threatens the right to privacy as both a human-security interest and a human right under Article 17 of the ICCPR.

Vietnam is confronting this tension as the government intensifies digital-transformation efforts and expands AI use across public-administration functions (Thanh, 2024). Under the National Digital Transformation Program, AI-enabled systems have been deployed in traffic management, crime prevention, and public-service delivery. Hanoi and Ho Chi Minh City operate extensive networks of AI-powered cameras capable of facial recognition, vehicle-plate identification, and real-time crowd monitoring. Although these systems improve administrative efficiency and public-order management, they also raise concerns regarding excessive data collection, unclear data-retention practices, and limited public understanding of how personal information is processed. Instances of surveillance images circulating online without consent further underscore the fragility of privacy protections in AI-driven environments (Nguyen, 2024)

As a socialist rule-of-law state committed to protecting human rights, Vietnam recognises privacy in its Constitution (2013) and has adopted several regulatory instruments, including the Civil Code (2015), the Law on Cybersecurity (2018), and Decree 13/2023/NĐ-CP on personal data protection. However, substantial regulatory gaps remain. Vietnam currently lacks an independent data-protection authority; national-security exemptions are broad; safeguards for automated decision-making are limited; and specific obligations for state agencies deploying AI surveillance are not clearly defined (Lâm, 2024) It therefore remains uncertain whether Vietnam's legal framework satisfies key ICCPR standards, particularly the requirements of legality, legitimate aim, necessity, and proportionality. Compared with rights-based regulatory models such as the EU's GDPR and South Korea's PIPA—both of which contain structured safeguards and enforceable individual rights—Vietnam's framework appears incomplete in addressing AI-specific privacy risks (Kim & Park, 2024; Malgieri & Comandé, 2017).

Despite the rapid adoption of AI surveillance in Vietnam, scholarly research remains limited. Existing studies tend to emphasise digital-government efficiency or general data-protection issues rather than the risks AI surveillance poses to privacy as a dimension of human security, or whether current laws adequately govern AI-specific threats. Systematic comparative analysis of Vietnam's emerging approach relative to established international models is also lacking.

This study responds to three key research gaps. First, there remains limited analysis of how AI-enabled surveillance may threaten the right to privacy as a core dimension of human security in Vietnam (UNDP, 1994). Second, there is insufficient evaluation of whether Vietnam's existing legal instruments—particularly Decree 13/2023/NĐ-CP and the Law on Cybersecurity—meet ICCPR requirements and can adequately regulate AI-specific privacy risks. Third, scholarship has not sufficiently clarified how Vietnam's emerging governance framework differs from international

human-centred, rights-based regulatory models such as the EU's GDPR and South Korea's PIPA, leaving a gap in comparative insight that could inform feasible reform pathways.

To address these gaps, the article aims to (i) examine the risks that AI surveillance poses to privacy as both a human-security interest and a human right protected by the ICCPR; (ii) assess the adequacy of Vietnam's legal framework for governing AI-driven surveillance using ICCPR-based criteria; and (iii) identify targeted lessons from international models that can support practical reforms balancing security objectives with meaningful privacy protection.

The study is guided by three research questions. RQ1 asks what risks AI-enabled government surveillance in Vietnam poses to the right to privacy, understood both as a core element of human security and as a human right protected under Article 17 of the ICCPR. This question focuses on surveillance practices such as facial recognition, biometric profiling, crowd analytics, and continuous behavioral tracking, examining how they may undermine individual autonomy, informational integrity, and personal safety, and how weak safeguards can produce disproportionate harms for vulnerable and marginalized groups. RQ2 asks the extent to which Vietnam's current legal framework satisfies ICCPR standards on privacy protection—legality, legitimate aim, necessity, and proportionality—and whether it provides adequate safeguards for emerging AI surveillance practices. This question assesses the normative and regulatory foundations of privacy in Vietnamese law, focusing on the Constitution (2013), Civil Code (2015), the Law on Cybersecurity (2018), and Decree 13/2023/NĐ-CP, and evaluates whether these instruments incorporate human-security principles and provide protections such as oversight, transparency, data minimization, and clear limits on biometric and automated monitoring. RQ3 asks what lessons from international regulatory models—particularly the GDPR and PIPA—can inform feasible legal reforms to enhance Vietnam's capacity to govern AI surveillance while safeguarding privacy and human security. This question conducts a focused comparison of two mature rights-based regimes to identify mechanisms such as independent data protection authorities, algorithmic transparency obligations, and impact assessment requirements, and then evaluates which elements could be adapted to Vietnam's legal and institutional context without undermining legitimate national-security aims.

Aligned with these questions, the research objectives are threefold. RO1 is to identify and analysis privacy risks posed by AI-enabled surveillance technologies in Vietnam—such as facial recognition, biometric profiling, crowd analytics, and behavioral tracking—through the lenses of human security and Article 17 of the ICCPR. RO2 is to assess whether Vietnam's constitutional and legislative framework, including Decree 13/2023/NĐ-CP and the Law on Cybersecurity, meets ICCPR standards of legality, legitimate aim, necessity, and proportionality in regulating AI surveillance. RO3 is to examine regulatory approaches under the GDPR and PIPA and extract lessons applicable to Vietnam for strengthening privacy protections and advancing human-center AI governance.

The study draws on four complementary theoretical perspectives to analyze the implications of AI surveillance for privacy rights and human security, evaluate Vietnam's legal framework, and derive comparative lessons. Privacy Rights Theory, grounded in international human rights law—particularly Article 17 of the ICCPR—conceptualizes privacy as protection against arbitrary or unlawful interference and as informational self-determination, emphasizing individuals' control over how personal data is collected, processed, and used (Bennett & Raab, 2017).

. This perspective provides the normative basis for assessing how AI surveillance practices may infringe autonomy and informational integrity (RQ1) and establishes the benchmark for evaluating Vietnam's legal compliance with legality, legitimate aim, necessity, and proportionality (RQ2). Human Security Theory, introduced by UNDP (1994), reframes security around individuals rather than states, emphasizing freedom from fear, freedom from want, and the right to live with dignity; within this frame, threats to autonomy, psychological safety, and social trust become central security concerns. This lens supports the analysis of how AI surveillance may restrict civic participation, deepen inequalities, and expose vulnerable groups to disproportionate monitoring, reinforcing privacy as essential to individual and societal well-being (RQ1). Digital Constitutionalism examines how constitutional principles—fundamental rights, transparency, proportionality, and checks and balances—should apply in digital governance environments where AI mediates state–citizen relations(Celeste, 2019). It therefore guides the assessment of whether Vietnam's constitutional and statutory safeguards meaningfully constrain state surveillance powers and provide rights-based accountability, including the need for independent oversight (RQ2).

Comparative Regulatory Theory, which studies how jurisdictions design legal and institutional responses to shared governance challenges, enables the identification of transferable principles and mechanisms (Baldwin et al., 2012). This perspective structures the comparative analysis of the GDPR and PIPA to identify actionable tools—such as independent regulators, algorithmic transparency, and mandatory impact assessments—that could be adapted to strengthen Vietnam's governance of AI-enabled surveillance (RQ3).

Together, these perspectives provide an integrated foundation for the study: Privacy Rights Theory and Human Security Theory clarify the nature and scope of privacy risks posed by AI surveillance (RQ1); Digital Constitutionalism supports the evaluation of Vietnam's legal framework against ICCPR and proportionality standards (RQ2); and Comparative Regulatory Theory informs the identification of feasible reforms drawing from the GDPR and PIPA (RQ3). This integrated approach enables a comprehensive, rights-based assessment of AI-enabled surveillance within Vietnam's socio-legal context.

Research Methods

The study adopts a qualitative research design that combines doctrinal legal analysis, comparative evaluation, and conceptual synthesis to examine the risks posed by AI-enabled surveillance, assess the adequacy of Vietnam's legal framework, and identify relevant lessons from international regulatory models. The methodological approach is grounded in the need to analyse privacy not only as a legal entitlement but also as an element of human security and an ICCPR-protected right.

Doctrinal analysis forms the core of the study. It involves a systematic interpretation of Vietnam's constitutional and statutory provisions governing privacy and surveillance. Key legal documents—including the 2013 Constitution, the Civil Code (2015), the Law on Cybersecurity (2018), the Law on Cyberinformation Security (2015), and Decree 13/2023/NĐ-CP—were selected through targeted keyword searches ("privacy," "surveillance," "biometric data," "AI governance," "automated monitoring") across official legal databases and government portals. These materials were analysed against Article 17 of the ICCPR and the principles of legality, legitimate aim, necessity, and proportionality developed in international human rights jurisprudence. This approach enables the identification of substantive gaps, inconsistencies, and areas

where domestic laws may fall short of safeguarding individuals from intrusive surveillance practices.

To complement the doctrinal method, the study incorporates a focused comparative analysis of two jurisdictions with mature regulatory frameworks for privacy and AI-related risks: the European Union's General Data Protection Regulation (GDPR) and South Korea's Personal Information Protection Act (PIPA). These legal systems were selected for their established safeguards regarding biometric data, automated decision-making, oversight mechanisms, and rights-based governance. The comparative method follows a functional approach, examining how these regimes address challenges associated with AI surveillance and identifying institutional or normative principles that may be adaptable to Vietnam's socio-legal context.

Conceptual synthesis is used to integrate insights from the theoretical frameworks of privacy rights, human security, digital constitutionalism, and comparative regulatory theory. These perspectives guide the interpretation of legal materials and policy documents, providing a holistic understanding of how AI-enabled surveillance affects individual autonomy, informational integrity, and constitutional protections.

The study relies exclusively on secondary sources, including peer-reviewed scholarship, legal commentaries, governmental reports, and publications from international organisations such as UNDP and the European Commission. Source selection prioritised relevance, credibility, and recency, particularly materials published after 2018 to reflect contemporary developments in AI technologies and data-protection governance.

Several limitations should be acknowledged. First, the study does not include interviews, surveys, or technical audits of AI systems; therefore, its assessment of lived experiences and operational practices depends on existing empirical and policy literature. Second, the reliance on doctrinal and comparative methods means that the analysis focuses on legal and normative dimensions rather than empirical measurement of surveillance impacts or algorithmic performance. Despite these limitations, the methodological design is appropriate for identifying legal and institutional gaps and for proposing reforms aligned with international human rights standards and human-security principles.

Results and Discussion

Overview of Artificial Intelligence (AI) Surveillance, Right to Privacy, and Human Security

Artificial intelligence (AI) surveillance has emerged as a defining feature of modern digital governance (Aloisit & Gramanott, 2019; Duberry, 2022; Dunleavy & Margetts, 2025). Across the world, governments increasingly rely on algorithmic tools—such as facial recognition, biometric identification, behavioural analytics, and automated decision-making—to monitor public spaces and support law-enforcement and administrative functions . This reflects the broader rise of algorithmic governance, in which decisions once made by human actors are delegated to computational systems that draw on vast, continuously expanding datasets (Yeung, 2018). In many smart-city deployments, these systems generate significant informational asymmetries: state and corporate actors accumulate large volumes of personal data, while individuals remain unaware of how such data are collected, used, or repurposed (Richards & Hartzog, 2015). This imbalance challenges informational self-determination and risks

normalizing pervasive surveillance as a routine component of everyday life (Zuboff, 2023)

Within this global context, the right to privacy functions as a foundational safeguard. International human rights law, reflected in Article 12 of the Universal Declaration of Human Rights (United Nations, 1948) and Article 17 of the International Covenant on Civil and Political Rights, prohibits arbitrary or unlawful interference with an individual's private life, home, family, or correspondence. The UN Human Rights Committee has further clarified that any interference with privacy must comply with the principles of legality, legitimate aim, necessity, and proportionality (UN Human Rights Committee, 2014). In this sense, privacy is not only about data protection, but also about safeguarding autonomy, dignity, and freedom from coercion in an era where digital technologies heighten the capacity for intrusive monitoring.

Understanding the implications of AI surveillance requires situating it within the framework of human security. Introduced by the United Nations Development Programme (UNDP, 1994), human security shifts attention from protecting the state to protecting individuals, emphasising "freedom from fear," "freedom from want," and "freedom from indignity." AI surveillance interacts with all three dimensions.

Freedom from fear is affected by the *chilling effect*, where individuals who know they are being monitored are more likely to self-censor or avoid civic participation—patterns documented among journalists, activists, and minority groups worldwide (Article 19, 2022). Freedom from want may be compromised when data collected for public-security purposes are reused in contexts such as employment screening, credit scoring, or welfare eligibility, leading to exclusion or unequal treatment (Lebovits, 2019). Freedom from indignity is threatened by algorithmic bias, which arises when AI systems trained on unrepresentative or skewed datasets reproduce or amplify discrimination against vulnerable groups (Buolamwini & Gebru, 2018). These insights reveal a clear conceptual chain that connects surveillance practices to broader concerns of governance and legitimacy: AI Surveillance → Informational Asymmetry → Privacy Erosion → Human Insecurity → Decline of Civic Trust (Richards & Hartzog, 2015; UNDP, 1994; Zuboff, 2023).

This model underscores that privacy risks associated with AI surveillance are not merely technical challenges; they are systemic issues affecting social stability, democratic participation, and public confidence in state institutions. As governments worldwide expand the use of AI technologies within public administration and national-security infrastructures, integrating human-security principles into regulatory frameworks becomes essential to ensure that technological advancements remain aligned with fundamental human-rights obligations.

Artificial Intelligence Surveillance's Risks of Violation of the Right to Privacy and Human Security in Vietnam

The expansion of AI-enabled surveillance in Vietnam presents profound and multidimensional risks to the right to privacy as both a human-security interest and an ICCPR-protected human right. Drawing on verified Vietnamese case examples and international scholarship, four interconnected dynamics emerge: informational opacity, behavioural chilling, algorithmic bias, and institutional accountability deficits. These dynamics do not operate in isolation; instead, they accumulate to reshape the lived experience of autonomy, dignity, and freedom from arbitrary state interference. Through the lens of human security, the severity of these risks becomes particularly

salient, revealing how AI surveillance can undermine citizens' psychological, social, and legal safety even in the absence of overt coercion.

Informational Opacity: The Rise of Unobservable Surveillance Power

Informational opacity reflects a structural condition in which AI surveillance generates high visibility for state authorities while remaining largely opaque to the individuals being monitored. The core problem is not simply the absence of public notices, but the lack of information necessary for foreseeability and contestability. In Hanoi, the Intelligent Operations Center deploys thousands of cameras with facial-recognition and behavioural-analysis functions, yet no public documentation clarifies data retention periods, cross-agency data sharing, or whether algorithmic outputs are subject to audit or review. Similarly, Ho Chi Minh City's AI-based traffic monitoring collects biometric and mobility data without publishing safeguards, impact assessments, or retention rules .

Opacity becomes especially problematic in AI contexts because surveillance no longer stops at recording observable events. As (Yeung, 2018) explains, algorithmic governance enables systems to infer behavioural patterns, risk categories, or social affiliations from raw data. Individuals may be aware that cameras exist, but they cannot reasonably foresee whether they are being identified, profiled, or cross-referenced with other databases, nor what consequences such inferences may trigger. This lack of predictability undermines the ICCPR requirement that interferences with privacy be lawful and non-arbitrary, as individuals cannot understand the scope, limits, or implications of state monitoring.

From a human-security perspective, informational opacity erodes privacy as informational autonomy and places individuals in a condition of continuous uncertainty. When people cannot know how their data is processed or whether algorithmic judgments are being made about them, they are exposed to data-driven decisions they cannot monitor or challenge. This uncertainty weakens personal agency and trust in public institutions, transforming opacity from a technical shortcoming into a structural threat to human security.

Behavioural Chilling: The Psychological Transformation of Civic Behaviour

AI surveillance in Vietnam increasingly operates as a behavioural constraint, producing what characterises as *modification under uncertainty*. Unlike traditional surveillance, AI-enabled systems amplify this effect by enabling continuous identification, retrospective analysis, and cross-referencing across time and space. Individuals may not know whether they are currently being monitored, but they are aware that their past actions can be reconstructed, classified, and evaluated later. This temporal uncertainty intensifies self-regulation and discourages lawful behaviour. Qualitative evidence suggests that such visibility triggers measurable behavioural change: journalists avoid recording near government buildings equipped with facial-recognition systems; participation in community dialogues declined after AI camera clusters were installed around public venues ; and civil-society organisations report that young activists increasingly refrain from protests or public discussion due to fears of retrospective identification.

These behavioural shifts go beyond individual discomfort and amount to a structural contraction of civic space. From a human-security perspective, they erode "freedom from fear," which underpins individuals' ability to participate in social and political life without psychological intimidation ((UNDP, 1994). Under the ICCPR,

surveillance that predictably leads individuals to suppress lawful expression, association, or movement—without a demonstrated and proportionate necessity—constitutes an indirect but substantive interference with private life and related freedoms. Importantly, this form of interference does not rely on overt coercion; it operates through anticipation and uncertainty. Over time, the chilling effect becomes self-reinforcing: as fewer people engage openly, restraint becomes the social norm, and silence emerges as a rational strategy for risk avoidance. In this way, AI-enabled surveillance reshapes collective behaviour and weakens the conditions necessary for human security, even in the absence of explicit repression

Algorithmic Bias: The Digital Amplification of Structural Inequalities

AI-enabled surveillance in Vietnam also raises significant concerns about algorithmic bias, particularly where systems are used for facial recognition, behavioural classification, or anomaly detection in public spaces. Algorithmic bias arises when AI systems systematically produce inaccurate or unequal outcomes due to the quality of training data, design assumptions, or contextual mismatch between the system and the social environment in which it operates. As global research shows, biometric and recognition systems often perform unevenly across different demographic groups, especially where training datasets are not representative or where "normal" behaviour is implicitly defined through narrow technical parameters (Buolamwini & Gebru, 2018) : (Lebovits, 2019)).

In the Vietnamese context, these risks are amplified by the way AI surveillance is deployed in densely populated urban areas and public-service environments. Anomaly-detection and behavioural-analysis systems are often designed to flag deviations from predefined patterns of movement or conduct. However, such systems struggle to distinguish between genuinely risky behaviour and socio-economic vulnerability. Reports from Bình Dương and Đà Nẵng indicate that migrant workers and homeless individuals were incorrectly flagged as "suspicious" based on movement patterns rather than unlawful conduct. These misclassifications illustrate how algorithmic systems can translate social marginality into digital risk, exposing already vulnerable groups to heightened scrutiny.

From an ICCPR perspective, algorithmic bias undermines the requirement that interferences with privacy be non-arbitrary. Surveillance becomes arbitrary not only when it lacks legal basis, but when its application produces inconsistent or discriminatory outcomes that are not reasonably foreseeable by those affected. Individuals subjected to algorithmic profiling often have no way of knowing why they were flagged, what data contributed to the decision, or how to challenge the outcome. In the absence of transparency and review mechanisms, biased outputs are treated as neutral or objective, masking discretionary power behind technical processes.

From a human-security perspective, algorithmic bias threatens dignity and equality by concentrating surveillance burdens on specific groups. When AI systems repeatedly misidentify or over-monitor certain populations, they generate a climate of unequal vulnerability and reinforce existing social hierarchies. This not only increases the risk of unjustified intervention, but also deepens feelings of exclusion and insecurity among those already at the margins. Over time, such patterns erode trust in public institutions and weaken the sense of safety and fairness that human security seeks to protect.

Taken together, algorithmic bias illustrates that AI surveillance risks are not evenly distributed across society. Without safeguards for transparency, contestability,

and institutional review, AI systems can reproduce and intensify structural inequalities, transforming technological error into a persistent source of human insecurity and a substantive violation of Article 17 of the ICCPR.

Institutional Accountability Deficits: The Structural Enabler of Systemic Risk

The most serious privacy threat arising from AI-enabled surveillance in Vietnam is not technological but institutional. While AI systems introduce risks of opacity, behavioural control, and bias, these risks become systemic precisely because Vietnam lacks an independent data protection authority capable of supervising surveillance deployments, conducting audits, or providing remedies. Decree 13/2023/NĐ-CP establishes baseline obligations for data processors, yet it does not mandate algorithmic impact assessments, transparency reporting, or procedural safeguards allowing individuals to contest automated decisions or misidentification outcomes (Lâm, 2024) Oversight functions are instead dispersed across multiple ministries, many of which are simultaneously responsible for deploying and regulating surveillance technologies. This institutional configuration blurs accountability and creates inherent conflicts of interest.

The absence of a dedicated supervisory body transforms legal safeguards into formal abstractions. Without independent oversight, requirements relating to legality, necessity, or proportionality lack an enforcement anchor. Informational opacity persists because no authority is tasked with demanding disclosure of retention rules or algorithmic logic. Behavioural chilling remains unaddressed because individuals have no avenue to challenge surveillance practices that suppress lawful conduct. Algorithmic bias goes uncorrected because no institution possesses both the mandate and technical capacity to audit AI systems or review discriminatory outcomes. In this way, institutional weakness does not merely coexist with other risks; it amplifies and entrenches them, allowing surveillance harms to accumulate unchecked.

From an ICCPR perspective, this institutional vacuum is decisive. Article 17 requires not only that interferences with privacy be grounded in law, but that they be accompanied by effective safeguards and accessible remedies. Where individuals cannot seek independent review, obtain explanations, or trigger corrective action, privacy protection exists largely on paper. As (Celeste, 2019) observes, governance gaps of this kind enable AI systems to operate as instruments of unchecked discretionary power, shielded by technical complexity and administrative opacity. In the context of AI surveillance, the lack of institutional oversight therefore constitutes a structural failure: it is the point at which otherwise correct legal principles lose their protective function and become incapable of preventing arbitrary interference with private life.

The four risk dynamics interact through a cumulative sequence:

Opacity → Fear → Bias → No Remedy → Human Insecurity

(i) Opacity creates unobservable forms of monitoring and inference.
(ii) Fear suppresses expression and participation.
(iii) Bias disproportionately harms already vulnerable populations
(iv) Lack of oversight ensures these harms cannot be challenged.

This sequence reveals that AI surveillance in Vietnam can transform privacy violations from episodic incidents into structural conditions that undermine autonomy, dignity, and trust—core values of human security and key purposes of Article 17 ICCPR.

The findings under RQ1 therefore establish essential groundwork for RQ2, which evaluates whether Vietnam's existing legal framework meets the ICCPR standards of legality, legitimate aim, necessity, proportionality, and institutional oversight.

Table 1. The Structural Enabler of Systemic Risk

Risks	Mechanism of Harm	Human Security Impact	ICCPR Article 17 Implications
Informational Opacity	Unobservable data processing; hidden algorithmic inference; loss of transparency	Loss of informational autonomy; inability to predict how data is used	Violates foreseeability and legal certainty requirements
Behavioural Chilling	Self-censorship driven by perceived monitoring; altered civic behaviour	Weakens freedom from fear; reduces civic participation	Disproportionate interference with private life and expression
Algorithmic Bias	Misclassification of vulnerable groups; context-blind anomaly detection	Reinforces inequality; increases exposure to policing	Arbitrary or discriminatory interference prohibited by ICCPR
Institutional Accountability Deficit	Lack of independent oversight; no redress mechanisms; fragmented authority	Institutional insecurity; inability to contest harm	Breach of safeguard and remedy obligations

Source: processed by author

Legal Adequacy of Vietnam's Framework Governing AI Surveillance

Evaluating whether Vietnam's legal framework adequately governs AI-enabled surveillance requires examining the extent to which existing laws meet the standards established under Article 17 of the ICCPR—namely legality, legitimate aim, necessity, and proportionality—as well as the broader principles of transparency and effective oversight. While Vietnam has formally recognised privacy rights through the Constitution (2013), Civil Code (2015), the Law on Cyberinformation Security (2015), the Law on Cybersecurity (2018), and most recently Decree 13/2023/NĐ-CP on Personal Data Protection, a closer analysis reveals significant normative and institutional gaps. These gaps raise concerns regarding whether current regulations are capable of addressing the specific risks posed by AI-driven surveillance technologies, particularly facial recognition, behavioural analytics, and biometric identification systems.

Legality: Absence of Clear, Accessible, and Predictable Legal Standards

The legality principle requires that any interference with privacy be grounded in legal rules that are clear, accessible, and foreseeable, so that individuals can understand in advance when and how the State may intrude into their private life and can adjust their conduct accordingly. Foreseeability, in this sense, is not satisfied merely because a country has laws mentioning privacy or cybersecurity. It requires that the law delineate, with sufficient precision, the scope of surveillance powers, the categories of data that may be collected, the conditions and procedures for collection, and the safeguards and remedies available to those affected. Without these elements, surveillance may formally appear "legal" yet remain effectively unpredictable to citizens, increasing the risk of arbitrary interference prohibited by Article 17 of the ICCPR.

Vietnam's legal instruments recognise privacy as a protected right, yet the scope and limits of state surveillance powers remain insufficiently defined in ways that are especially problematic for AI-enabled monitoring. The Law on Cybersecurity (2018) authorises state agencies to protect national cyberspace and maintain public order, but it does not articulate AI-specific procedural safeguards for surveillance tools that

operate through facial recognition, behavioural analytics, or automated profiling. In particular, the law does not clarify what constitutes a valid lawful basis for collecting and processing biometric identifiers, which are intrinsically sensitive and uniquely capable of enabling continuous identification in public spaces. As a result, biometric surveillance can be justified through broad references to security functions without clear statutory thresholds governing when such collection is permitted, how it must be limited, or what safeguards must accompany it.

Decree 13/2023/NĐ-CP represents an important step toward personal data protection, but it remains primarily a general processing framework and does not clearly distinguish between ordinary data processing and high-risk AI surveillance. In practice, this matters because AI surveillance differs not only in scale but in function: it enables continuous monitoring, "inference" of behavioural patterns, and retrospective identification. Yet Decree 13 does not create a high-risk category that would trigger heightened obligations for technologies such as facial recognition in public spaces, nor does it prescribe mandatory procedures tailored to AI-driven monitoring. Critically, Vietnam's framework also lacks legally required Data Protection Impact Assessments (DPIAs) or equivalent mechanisms that would force agencies to document the necessity, proportionality, and safeguards of high-risk surveillance before deployment. Without impact assessments, the legality of surveillance rests largely on administrative discretion rather than structured legal justification.

The legality deficit is compounded by the limited transparency surrounding actual deployments. AI surveillance systems in Hanoi and Ho Chi Minh City operate without publicly disclosed rules on data retention, cross-agency data sharing, access control, or algorithmic inference . This creates a practical foreseeability problem: even if citizens know cameras exist, they cannot reasonably predict whether their biometric images will be retained for days or years, whether the data will be merged with other administrative databases, or whether automated systems will generate "risk" classifications based on their movements. In ICCPR terms, the interference becomes difficult to contest because the legal and procedural contours of surveillance remain opaque to those affected.

Taken together, these shortcomings suggest that Vietnam's framework does not yet satisfy the legality standard required by Article 17 ICCPR in the specific context of AI surveillance. The challenge is not that Vietnam lacks laws, but that existing laws do not provide sufficiently precise, accessible, and technology-sensitive rules to ensure predictability, constrain discretion, and prevent arbitrary interference—especially where biometric identification and automated monitoring are involved.

Legitimate Aim: Broad and Vague Justifications Enable Discretionary Expansion

Vietnamese laws commonly justify AI surveillance through references to "public security," "social order," and "national security." While such aims may be legitimate under the ICCPR, their breadth and vagueness create space for expansive interpretation.

For instance, AI traffic monitoring is justified to enhance administrative efficiency, but the systems collect facial images and behavioural data that far exceed what is strictly needed for traffic enforcement . Similarly, facial-recognition deployment in administrative zones is justified for "public safety," yet no evidence suggests that less intrusive measures were considered.

Without statutory thresholds or specificity, legitimate aims risk becoming catch-all justifications, granting authorities significant discretion to broaden surveillance scope without proportional safeguards.

Vietnamese laws commonly justify AI surveillance through references to "public security," "social order," and "national security." While these objectives are, in principle, capable of constituting legitimate aims under Article 17 of the ICCPR, their breadth and indeterminacy create a structural risk of overreach. Under international human rights law, a legitimate aim must not only be formally acceptable but also sufficiently specific to constrain state discretion. When legal objectives are framed in overly general terms, they cease to function as meaningful limits and instead become flexible labels that can be stretched to accommodate a wide range of surveillance practices.

This problem is evident in the deployment of AI systems in Vietnam. AI-based traffic monitoring is often justified on grounds of administrative efficiency and public safety, yet the technical design of these systems enables the collection of facial images, behavioural patterns, and movement trajectories that go far beyond what is strictly necessary to identify traffic violations. The expansion of data collection from vehicle-related information to biometric and behavioural data illustrates how a broadly stated aim can gradually absorb additional surveillance functions without renewed legal justification. Similarly, facial-recognition systems installed in administrative or public-service areas are justified under the banner of "public safety," but there is little evidence that authorities have systematically assessed whether less intrusive alternatives—such as non-biometric access control or manual verification—could achieve the same objectives.

From an ICCPR perspective, this dynamic undermines the legitimate-aim requirement by allowing mission creep. When surveillance measures are justified by open-ended objectives, it becomes difficult to distinguish between what is genuinely required to achieve a lawful aim and what reflects discretionary expansion driven by technological capability rather than necessity. The absence of statutory thresholds specifying which surveillance tools may be used for which purposes, and under what conditions, means that legitimate aims risk functioning as catch-all justifications rather than as substantive constraints on state power.

The legal consequence is that surveillance may remain formally tied to a "legitimate aim" while becoming substantively disproportionate. Without clear purpose limitation, authorities retain wide discretion to broaden the scope of AI surveillance, collect additional categories of data, and repurpose information for secondary uses, all under the same general justification. This weakens the protective function of the legitimate-aim requirement and increases the likelihood of arbitrary interference with privacy, contrary to the object and purpose of Article 17 ICCPR.

Necessity: Lack of Evidence Demonstrating Minimal-Intrusion Approaches

The ICCPR requires that any interference with privacy be strictly necessary to achieve a legitimate objective, which implies that the State must demonstrate not only that a measure pursues a lawful aim, but also that no less intrusive alternative would be capable of achieving that aim with comparable effectiveness . Necessity therefore functions as a substantive constraint on state power, obliging authorities to justify why highly intrusive surveillance technologies, particularly biometric and AI-driven systems, are indispensable rather than merely convenient or technologically attractive.

Vietnamese law does not currently impose such a requirement. There is no statutory obligation for state agencies to demonstrate the necessity of AI-powered

surveillance, to compare AI-based monitoring with less intrusive alternatives (such as manual supervision, non-biometric sensors, or anonymised data collection), or to substantiate their choices through risk, impact, or necessity assessments. As a result, the decision to deploy AI surveillance is largely discretionary and driven by administrative efficiency or technological availability rather than by evidence-based evaluation of necessity.

This gap is evident in the adoption of facial-recognition technologies for crowd management and so-called "anomaly detection" in urban areas. These systems are frequently justified as tools to enhance public safety or administrative efficiency, yet there is little publicly available evidence showing that they outperform traditional policing methods, targeted patrols, or manual review in preventing disorder or identifying genuine threats. The absence of empirical benchmarking is particularly problematic given the intrusive nature of biometric surveillance, which enables continuous identification and tracking in public spaces.

The necessity deficit becomes more pronounced when considering documented errors. In Bình Dương and Đà Nẵng, AI-based anomaly-detection systems reportedly misidentified migrant workers and homeless individuals as "suspicious," despite the absence of unlawful behaviour. Such outcomes illustrate that intrusive technologies may not only be unnecessary but also counterproductive, generating false positives that divert law-enforcement resources and disproportionately affect vulnerable groups. From a necessity perspective, the deployment of systems that produce significant error rates raises serious doubts as to whether they are genuinely required to achieve the stated objective.

In ICCPR terms, the failure to assess necessity transforms AI surveillance from a carefully justified measure into a default governance tool, deployed without demonstrating that it is indispensable. When less intrusive alternatives are neither considered nor ruled out, the requirement of necessity collapses into a formal assertion rather than a substantive safeguard. This significantly increases the risk of arbitrary interference with privacy and undermines the protective function of Article 17, particularly in contexts where AI surveillance operates at scale and affects large segments of the population.

Proportionality: Lack of Constraint on Scope, Duration, and Intrusiveness

The proportionality requirement under international human rights law demands that surveillance measures be narrowly tailored to the legitimate aim pursued and that the intrusion into privacy be limited to what is strictly necessary in scope, duration, and intensity (UN Human Rights Committee, 2014). Proportionality thus operates as a second-order safeguard: even where surveillance is lawful and pursues a legitimate objective, it must still be constrained so that the degree of intrusion does not exceed the actual needs of that objective. In the context of AI-enabled surveillance, this principle is particularly important because such systems enable continuous monitoring, large-scale data aggregation, and long-term storage, all of which amplify the potential harm to privacy.

Vietnam's legal framework currently lacks several core elements required to operationalise proportionality. There are no clear statutory limits on how long biometric data may be retained, no binding rules restricting the geographic or functional scope of AI surveillance, and no prohibitions on secondary uses of data derived from AI systems. Moreover, Vietnamese law does not contain procedural requirements governing the deployment of high-risk AI technologies, such as facial recognition or behavioural

analytics, that would oblige authorities to justify the scale or duration of surveillance in relation to the specific aim pursued. In the absence of such constraints, AI surveillance risks becoming structurally excessive, not because of a single unlawful act, but because of cumulative over-collection and prolonged retention.

This problem is illustrated by smart-city surveillance systems in major Vietnamese cities, which continuously record movement, behavioural patterns, and, in some cases, biometric identifiers without publicly disclosed retention timelines or criteria for data . Indefinite or open-ended retention of biometric data is difficult to reconcile with proportionality, as it extends surveillance effects far beyond the immediate purpose for which the data was collected. Over time, retained data may be repurposed, combined with other datasets, or accessed by additional agencies, exposing individuals to ongoing risks of misuse, unauthorised access, or secondary profiling that were not envisaged at the time of collection.

From an ICCPR perspective, the absence of proportionality safeguards creates conditions in which surveillance measures, although initially justified, gradually expand in both scope and impact. This phenomenon—often described as function creep—undermines the core logic of proportionality by allowing a measure designed for a limited objective to evolve into a general monitoring infrastructure. Without clear legal limits on retention, scope, and reuse, authorities retain broad discretion to intensify surveillance without renewed justification or review. The result is a regulatory environment in which highly intrusive AI systems can be deployed broadly and persistently, affecting large segments of the population without a demonstrated need or clearly defined boundaries.

In practical terms, this means that proportionality in Vietnam remains largely aspirational rather than operational. Even if surveillance serves a legitimate aim, the lack of enforceable constraints allows privacy interference to exceed what is necessary, rendering the safeguard ineffective. Such conditions are incompatible with ICCPR standards, which require that surveillance be continuously justified and recalibrated to prevent excessive intrusion. Without explicit proportionality rules and mechanisms to enforce them, AI-enabled surveillance in Vietnam risks normalising overbroad and enduring intrusions into private life, contrary to the object and purpose of Article 17.

Oversight and Remedies: The Structural Gap Undermining All Safeguards

Beyond legality, necessity, and proportionality, the ICCPR requires that any interference with privacy be accompanied by effective safeguards and accessible remedies. These elements are not ancillary; they are constitutive of the right itself. Under international human rights doctrine, a privacy regime that recognises limits on paper but fails to provide mechanisms for supervision, review, and redress does not satisfy Article 17, because individuals remain unable to challenge or correct unlawful or disproportionate interferences.

This is the area in which Vietnam's framework is most deficient. Vietnam currently has no independent data protection authority with the legal mandate and institutional autonomy to investigate, audit, sanction, or monitor AI-enabled surveillance practices. Oversight responsibilities are dispersed among several ministries—most notably the Ministry of Public Security and the Ministry of Information and Communications—whose mandates often overlap and whose roles combine both implementation and supervision functions. This institutional configuration blurs lines of accountability and creates inherent conflicts of interest, as the same agencies

responsible for deploying surveillance technologies are also expected to regulate their use (Lâm, 2024).

Decree 13/2023/NĐ-CP, while introducing important baseline obligations for personal data protection, does not remedy this structural weakness. It provides no clear procedure through which individuals can challenge algorithmic decisions, contest misidentification, or seek redress for data misuse arising from AI surveillance. Nor does it designate a competent authority to receive complaints, conduct independent investigations, or issue binding corrective orders. In practical terms, individuals affected by facial-recognition errors, behavioural profiling, or secondary data use lack a clear legal pathway to assert their rights.

This absence of oversight and remedies magnifies all other shortcomings identified in RQ2. Even if Vietnam were to strengthen legal bases, narrow legitimate aims, and introduce necessity and proportionality tests, these safeguards would remain largely symbolic without an institution capable of enforcing them. The risk is that compliance becomes discretionary, dependent on administrative goodwill rather than legal obligation. Under ICCPR jurisprudence, such a framework constitutes a structural violation of Article 17, because it fails to ensure that privacy protections are effective in practice and accessible to those whose rights are affected.

In the context of AI-enabled surveillance, the consequences are particularly severe. Automated systems operate at scale, generate errors that may not be immediately visible, and produce harms—such as misidentification or discriminatory profiling—that require prompt correction. Without independent supervision and remedies, these harms can persist unchecked, normalising intrusive surveillance and eroding public trust. From a human security perspective, the absence of enforceable remedies undermines individuals' sense of control, dignity, and safety in digital spaces.

Accordingly, strengthening oversight and remedy mechanisms is not merely an institutional reform but a precondition for the effectiveness of all other safeguards. Without independent supervision and accessible redress, Vietnam's AI surveillance framework cannot meet the requirements of Article 17 ICCPR, regardless of how well legality, necessity, or proportionality are articulated in law.

Table 2. ICCPR Privacy Standards and Vietnam's Legal Compliance Assessmen

ICCPR Standard	Requirements	Vietnam's Legal Position	Assessment
Legality	Laws must be clear, accessible, and foreseeable	Privacy laws exist but lack specificity; no DPIA requirements; opaque AI deployments	Partially compliant but insufficient clarity
Legitimate Aim	Must be specific and demonstrable	Security and public-order aims broadly defined; vague justifications	Weak compliance due to broad legal bases
Necessity	Interference must be strictly required; alternatives assessed	No necessity tests; no requirement to consider less intrusive options	Non-compliant
Oversight/Remedies	Effective, independent oversight must exist	No independent DPA; fragmented institutional responsibility; no remedy mechanism	Non-compliant (critical gap)

Source: processed by author

Comparative International Experiences in Safeguarding the Right to Privacy and Human Security in AI Surveillance Contexts

As governments worldwide confront the rapid expansion of AI-enabled surveillance, the European Union and South Korea have built two of the most mature and operationally effective privacy frameworks in response to growing concerns over biometric monitoring, automated profiling, and data-driven governance. The EU adopted the General Data Protection Regulation (GDPR) in 2016 against the backdrop of rising commercial data exploitation and the increasing use of algorithmic systems across sectors. GDPR established a harmonised, rights-based regulatory framework emphasising strict limits on biometric processing, clear legal bases for high-risk technologies, and strong protections against automated decision-making South Korea's Personal Information Protection Act (PIPA), enacted in 2011 and substantially strengthened between 2020 and 2023, emerged from Korea's rapid digital transformation, high internet penetration, and repeated data-breach scandals. PIPA now forms one of Asia's strongest privacy regimes, with enhanced safeguards for sensitive data, explicit rules for algorithmic processing, and strengthened user rights.

A defining feature of both GDPR and PIPA is not merely the substantive rules they contain, but the institutional machinery that ensures these rules have practical force. Under GDPR, enforcement is decentralised through a network of independent Data Protection Authorities (DPAs), each authorised to audit AI systems, investigate non-compliance, suspend unlawful processing, and impose administrative penalties. Protection Board, ensuring harmonised interpretation and cross-border enforcement. In South Korea, oversight is centralised in the Personal Information Protection Commission (PIPC), a fully independent authority empowered to regulate both public and private sectors, conduct inspections, issue corrective orders, and intervene in high-risk or discriminatory AI deployments. These institutions convert legal norms into enforceable constraints and create a regulatory environment where intrusive technologies are subject to real scrutiny.

For Vietnam, which is expanding AI surveillance rapidly—particularly in smart-city governance, traffic monitoring, and public-security applications—but still lacks a unified, rights-protective governance structure, GDPR and PIPA offer valuable sources of reference. Their relevance does not lie in their complexity but in their alignment with developmental conditions similar to Vietnam's: high levels of digital adoption, ambitious e-government agendas, dense urban environments, and strong central-state coordination. South Korea, in particular, shares several socio-economic and administrative characteristics with Vietnam, including a strong executive, rapid digital innovation, and large-scale state-led data infrastructures. Both GDPR and PIPA also respond to concerns that mirror Vietnam's current trajectory—balancing digital

that it is possible to regulate intrusive technologies in a manner consistent with Article 17 of the ICCPR while still advancing national-security objectives and digital transformation priorities.

Legal Foundations for Biometric Surveillance

GDPR responds to the legality gap through a carefully structured system of legal bases in Articles 6 and 9, which do more than simply "allow or prohibit" biometric processing. Article 6 sets out an exhaustive list of lawful grounds for any processing—such as consent, performance of a legal obligation, protection of vital interests, public interest, or legitimate interests—while Article 9(1) elevates biometric data used for identification into a "special category" that is presumptively prohibited. Only a small

number of exceptions in Article 9(2) can override this prohibition, and each exception must be grounded in a clear legal mandate and accompanied by appropriate safeguards. This structure ensures that biometric surveillance is not treated as a default technological option but as an exceptional interference with privacy that must be explicitly justified in law.

PIPA Article 23-2 follows the same logic in a different legal context. By defining biometric identifiers (such as fingerprints, facial geometry, or iris patterns) as "sensitive information," it requires that any processing rest on strict necessity and clearly stated purposes, and that additional safeguards—such as encryption, access controls, and minimisation—be applied . In practice, Korean ministries and local governments seeking to deploy biometric systems must frame their projects within these legal constraints and submit them to PIPC scrutiny, rather than relying on generic "security" rationales.

What makes these provisions effective is the institutional machinery that enforces them. In the EU, Data Protection Authorities (DPAs) do not merely receive notifications; they actively review whether controllers have properly identified a lawful basis under Articles 6 and 9, examine supporting documentation, and may suspend or prohibit processing that does not meet statutory requirements. Several DPAs have already ordered the shutdown or scaling-back of facial-recognition projects where no adequate legal basis existed. In South Korea, the PIPC performs a similar function: it evaluates whether agencies invoking a "lawful purpose" under PIPA have adequately justified the necessity and scope of biometric surveillance, and it can order deletion of unlawfully collected data or modification of processing practices when legal standards are not met.

By contrast, Vietnam currently lacks both explicit lawful bases for biometric surveillance and an independent institution capable of verifying whether those bases are satisfied. Authorities can invoke broad mandates such as "public security" without specifying concrete legal grounds, and no external body checks whether the collection and use of biometric data is genuinely necessary or proportionate. Borrowing the principle of legal specificity from GDPR and PIPA—explicitly listing lawful purposes for biometric use, defining biometric data as a sensitive category, and pairing these rules with a supervisory authority empowered to review compliance—would directly address the legality gap identified in RQ2. It would also move Vietnam closer to the ICCPR Article 17 standard, which requires that interferences with privacy be not only grounded in law, but sufficiently clear, foreseeable, and accompanied by effective safeguards.

Narrowing Security Justifications Through Institutional Review

In Vietnam, references to "public security" and "social order" currently operate as very broad legal justifications for AI surveillance. Because these terms are not further specified in legislation, they can be invoked to legitimise a wide range of monitoring practices—from traffic enforcement to crowd analytics and facial recognition in administrative areas—without any clear boundary on what is truly necessary or proportionate. This is precisely the kind of open-ended justification that Article 17 of the ICCPR warns against: an interference with privacy may pursue a legitimate objective, but if that objective is framed too vaguely, it becomes difficult to distinguish between necessary measures and discretionary expansion.

GDPR and PIPA handle this problem by tightening both the definition of purpose and the link between that purpose and the processing activity, and then subjecting that link to institutional review.

Under GDPR's purpose-limitation principle (Article 5(1)(b)), personal data—especially special categories such as biometric data—may only be collected for "specified, explicit and legitimate purposes" and cannot later be used in a manner incompatible with those purposes . That means a municipality in the EU cannot simply justify a facial-recognition system by citing "public safety" in general terms; it must show that the system is directed at a concrete, legally defined aim, such as identifying individuals on a terrorism watchlist, and that the scope of processing remains aligned with that precise aim. DPAs then examine whether the declared purpose is sufficiently specific, whether it fits within the legal mandate, and whether subsequent uses of the data respect that limitation.

South Korea's PIPA applies a similar logic. Public bodies must identify clear statutory bases and specific purposes when processing personal and especially sensitive information. When agencies cite reasons like "crime prevention" or "public safety," the PIPC is able to examine whether these labels correspond to a concrete policy goal rooted in law or are being used as broad rhetorical cover for expansive surveillance. Where justifications are overly general or the processing extends beyond what the purpose can reasonably support, PIPC can require narrowing of the project, impose conditions, or order corrective measures.

For Vietnam, the key lesson is that legitimate aim is not just a matter of drafting narrower phrases on paper; it is a matter of coupling clearer statutory purposes with an institution that can interrogate and test those purposes in practice. If "public security" continues to be used as a generic category, AI surveillance will remain vulnerable to mission creep and discretionary expansion. But if Vietnam defines more concrete aims in legislation—for example, limiting certain AI tools to the investigation of clearly enumerated offences or narrowly tailored safety functions—and equips a supervisory authority with the power to demand detailed justification and reject vague or pretextual uses of "public security", then the legitimate-aim requirement under ICCPR begins to operate as a real constraint rather than a formal label. This is how the second gap identified in RQ2—overbroad and under-specified aims—can be addressed in both normative and institutional terms.

Necessity and Proportionality in AI Surveillance Deployment

Vietnam currently has no statutory or procedural mechanism requiring state agencies to justify why intrusive AI systems—such as facial recognition, anomaly detection, or behavioural analytics—are necessary. As identified in RQ2, the absence of a necessity test allows authorities to deploy high-risk technologies simply because they are available, convenient, or technologically appealing, rather than because they are the least intrusive means capable of achieving a legitimate aim. This creates a significant misalignment with Article 17 of the ICCPR, which requires that any interference with privacy be not only lawful and purposeful but strictly necessary in a democratic society.

GDPR remedies this problem through Article 35, which mandates a Data Protection Impact Assessment (DPIA) whenever processing is "likely to result in a high risk to the rights and freedoms of natural persons." Importantly, the DPIA is not a self-certifying document. It obliges data controllers to identify the purpose of processing, evaluate whether less intrusive alternatives exist, assess potential harms, and outline mitigation measures. The effectiveness of the DPIA derives from the fact that DPAs have the authority to review these assessments, demand revisions, and—crucially—prohibit processing that cannot demonstrate necessity or adequate safeguards. DPAs

therefore function as a substantive check: they do not simply receive assessments but scrutinize the justifications contained within them.

South Korea's PIPA establishes a parallel structure through Article 28-2, requiring government entities and large-scale processors to conduct a Personal Information Impact Assessment (PIIA). The PIPC exercises an institutional review function similar to DPAs in Europe. It evaluates whether agencies have properly established necessity, whether the scope of processing is proportionate, and whether mitigation measures appropriately address risks. Where agencies fail to demonstrate necessity or where risks outweigh benefits, the PIPC can require revisions or halt deployment.

These institutional mechanisms ensure that necessity is not treated as a rhetorical justification but as an evidence-based regulatory standard. They operationalise necessity through a combination of: (i) a structured procedural tool (the DPIA/PIIA), and (ii) an empowered reviewer (DPAs/PIPC) who can interrogate necessity claims, require alternatives analysis, and disallow unjustified AI deployments.

Vietnam can realistically implement a streamlined, context-appropriate version of these impact assessments—focused specifically on high-risk AI systems—without replicating the full EU or Korean models. However, the effectiveness of such assessments hinges on the existence of an oversight body capable of reviewing them, because without institutional review, any assessment requirement becomes symbolic. A supervisory authority must be able to question necessity claims, request additional evidence, and reject deployments where less intrusive alternatives are available.

This combined approach—a procedural necessity test paired with institutional oversight—would directly close the necessity gap identified in RQ2. It would also bring Vietnam significantly closer to compliance with international standards by ensuring that intrusive AI surveillance technologies are deployed only when genuinely required, justified through evidence, and proportionate to the legitimate aim pursued.

Limiting Intrusiveness Through Institutional Monitoring

Proportionality requires that any interference with privacy be strictly limited in scope, duration, and intensity, and that surveillance activities do not extend beyond what is necessary to achieve a clearly defined aim.

Under the GDPR, this principle is given real operational effect through multiple substantive requirements—data minimisation, purpose limitation, retention limits, and restrictions on secondary use—combined with institutional mechanisms that ensure these requirements are not ignored in practice. DPAs routinely carry out audits to verify whether organisations have collected more data than necessary, retained it longer than justified, or repurposed it in a manner inconsistent with the original aim. When disproportionate practices are identified, DPAs may order deletion, restrict processing, or impose administrative penalties, transforming proportionality from a legal aspiration into an enforceable standard.

South Korea's PIPA embeds similar safeguards through requirements that data collection be reduced to the minimum necessary and that retention periods be clearly defined and justified. What distinguishes the Korean model, however, is the capacity of the Personal Information Protection Commission (PIPC) to monitor compliance through on-site inspections, detailed reviews of retention schedules, and corrective orders requiring agencies to narrow the scope of surveillance or cease secondary uses. PIPC's independence and its technical units dedicated to assessing database practices enable

it to detect and rectify proportionality breaches, including those arising from AI and biometric systems.

Vietnam's framework, as outlined in RQ2, contains none of these structural safeguards. There are no statutory limits on how long biometric data may be retained, no requirements to justify the breadth of data collection, and no restrictions on function creep—the gradual expansion of data use beyond its original purpose. Indeed, the smart-city systems deployed in Hanoi and Ho Chi Minh City collect continuous streams of behavioural and mobility data without any disclosed retention timelines or secondary-use prohibitions. Even if Vietnam were to introduce proportionality clauses into legislation, such clauses would be ineffective without an institution capable of verifying compliance, reviewing retention schedules, and intervening when surveillance exceeds necessity.

The transferable lesson from GDPR and PIPA is therefore not limited to adopting proportionality language, but to establishing the institutional capacity required to enforce it. Proportionality becomes operational only when a supervisory authority is empowered to: (i) examine whether collected data exceeds what is necessary; (ii) review retention practices for excessive duration; (iii) investigate secondary uses of AI-generated data; and (iv) sanction violations when processing becomes disproportionate.

Without such institutional machinery, any proportionality obligation would remain largely symbolic. For Vietnam, building proportionality into AI governance thus requires both normative precision and institutional enforcement power. Creating a supervisory mechanism capable of auditing AI systems, reviewing proportionality assessments, and mandating corrective measures is essential to closing the proportionality gap identified in RQ2 and ensuring that intrusive surveillance technologies do not erode privacy protections guaranteed under Article 17 of the ICCPR.

Independent Supervision and Accessible Remedies

Oversight remains the most critical structural gap in Vietnam's current legal framework. As detailed in RQ2, Vietnam has neither an independent supervisory authority nor a coherent enforcement mechanism capable of reviewing AI surveillance deployments, evaluating their legality or proportionality, or providing remedies to citizens whose privacy has been infringed. In contrast, the effectiveness of both the GDPR and PIPA is rooted in the institutional machinery that ensures privacy rules are continuously monitored, interpreted, and meaningfully enforced.

Under the GDPR, Articles 51–59 establish Data Protection Authorities (DPAs) in every Member State as independent regulators with the legal autonomy and technical expertise to conduct investigations, audit biometric and AI systems, suspend or prohibit unlawful processing, impose administrative fines, mediate complaints, and compel compliance with necessity–proportionality obligations. DPAs also coordinate through the European Data Protection Board (EDPB), which harmonises regulatory practice and strengthens the capacity of national authorities to supervise complex, cross-border technologies. This multilayered oversight infrastructure ensures that individuals' rights are not merely articulated in legal text but are actively protected through institutional scrutiny.

South Korea's model, while more centralised, is equally robust. The Personal Information Protection Commission (PIPC)—elevated to full independence in 2020—operates as the country's primary authority for privacy and AI governance. The PIPC's

powers include conducting on-site inspections of government surveillance systems, ordering the suspension or modification of unlawful processing, adjudicating complaints, issuing corrective recommendations, and imposing sanctions for non-compliance. Its independence from the executive branch, combined with its technical units specialising in AI and sensitive-data processing, allows it to function as an impartial and capable regulator of rapidly evolving technologies.

Vietnam lacks any such institution. Oversight is dispersed across multiple ministries with overlapping mandates, producing a fragmented system that is ill-suited to supervise AI deployments or ensure accountability. There is no authority empowered to audit facial-recognition systems in Hanoi or Ho Chi Minh City, assess proportionality in smart-city deployments, investigate algorithmic misclassification, require remedies, or order suspension of non-compliant processing. The absence of a unified and independent supervisory mechanism means that even well-drafted legal provisions would remain largely symbolic, with no operational force behind them. This structural weakness poses a clear risk of arbitrary or disproportionate interference with privacy, incompatible with Article 17 of the ICCPR, which requires not only safeguards in law but effective oversight and accessible remedies.

The central lesson from the GDPR and PIPA, therefore, is that privacy protection hinges on institutional capacity. A supervisory authority must possess: (i) independence to avoid conflicts of interest; (ii) investigatory powers to examine AI systems directly; (iii) sanctioning authority to compel compliance; (iv) complaint-handling mechanisms to provide remedies to individuals; and (v) technical expertise to understand algorithmic and biometric systems.

Vietnam can realistically adapt this model by establishing a functionally independent supervisory body—whether as a new institution or as a semi-autonomous unit within an existing ministry—provided it is granted statutory autonomy, enforcement authority, and adequate resources. Such an institution would fill the oversight and remedies gap identified in RQ2 and form the institutional backbone required for Vietnam to ensure that AI-enabled surveillance complies with both domestic constitutional principles and its international commitments under the ICCPR.

Table 3. Comparative Privacy Governance for AI and Biometric Surveillance: GDPR, PIPA, and Gaps in Vietnamese Law

Dimension	EU – GDPR	Korea – PIPA	Vietnamese law's gaps
Core regulatory focus	Rights-based framework with strict limits on biometric processing, clear lawful bases, purpose limitation, and safeguards against automated decision-making	Comprehensive protection of personal and sensitive data, with explicit rules for biometrics and algorithmic processing	Fragmented regulation across Constitution, Civil Code, cybersecurity laws, and Decree 13/2023; no AI-specific framework
Legal foundations for biometric surveillance	Articles 6 & 9: exhaustive lawful bases; biometric data as "special category"; presumptive prohibition with narrow exceptions	Article 23-2: biometric identifiers as "sensitive information"; strict necessity and purpose limitation	No explicit lawful bases for biometric surveillance; broad reliance on "public security"

Legitimate aim (purpose limitation)	Article 5(1)(b): processing only for specified, explicit, and legitimate purposes; enforced through DPA review	Clear statutory purposes required; PIPC reviews whether aims are concrete or pretextual	"Public security" and "social order" used as catch-all justifications
Necessity assessment	Article 35 DPIA required for high-risk processing; DPAs review and can block unjustified deployments	Article 28-2 Personal Information Impact Assessment; PIPC evaluates necessity and risk mitigation	No requirement to demonstrate necessity or consider less intrusive alternatives
Proportionality safeguards	Data minimisation, retention limits, restrictions on secondary use; enforced via DPA audits	Minimal collection, defined retention periods, inspections by PIPC	No statutory retention limits; no controls on function creep
Institutional machinery (oversight)	Independent Data Protection Authorities (Arts. 51–59); coordinated by EDPB; audit, sanction, suspend processing	Centralised, independent PIPC with investigatory, corrective, and sanctioning powers	Fragmented oversight across ministries; no independent supervisory authority
Algorithmic accountability	Article 22 & Recital 71: limits on automated decisions; DPAs audit algorithms and require safeguards	Articles 30 & 36: transparency, accuracy, correction rights; PIPC conducts technical inspections	No rules on automated decision-making or algorithmic audits
Remedies and enforcement	Complaints handled by DPAs; binding decisions; fines; judicial review	Complaint resolution, corrective orders, sanctions by PIPC	No clear mechanism for individuals to challenge AI surveillance harms

Source: processed by author

Proposals for Enhancing Vietnam's Legal Framework on Safeguarding Privacy and Human Security in the Context of AI Surveillance

Building on the comparative analysis of the EU's GDPR and South Korea's PIPA, it becomes clear that Vietnam's current framework is constrained not only by substantive legal gaps but also by the absence of institutional mechanisms capable of giving those rules practical effect. As identified in RQ2, these shortcomings include unclear legal bases, overly broad justifications for surveillance, the lack of necessity and proportionality review, and weak arrangements for independent oversight and remedies. The experiences of the EU and South Korea demonstrate that such gaps cannot be addressed through abstract legal principles alone, but require phased regulatory design, sector-specific governance tools, and enforceable institutional arrangements.

Accordingly, the following recommendations are presented as a progressive reform pathway that translates these comparative lessons into context-sensitive and politically feasible measures for Vietnam. Rather than advocating abrupt or idealised reform, the proposed approach recognises Vietnam's legal culture, administrative

capacity, and political–institutional conditions, and structures reform across short-, medium-, and long-term phases to gradually strengthen privacy protection and human security while preserving policy stability and governance effectiveness.

Short-Term Measures (1–2 years): Sectoral Guidance, DPIA/AIA Pilots, and Transparency Standards

In the short term, Vietnam can take meaningful steps without major institutional restructuring. The most urgent priority is to introduce structured necessity–proportionality review for high-risk AI surveillance, particularly in sectors where deployment is already advanced, such as smart-city management, traffic enforcement, and public security.

A practical and feasible measure is the issuance of sector-specific guidance on Data Protection Impact Assessments (DPIAs) or Algorithmic Impact Assessments (AIAs). These guidelines should be developed jointly by the Ministry of Information and Communications and the Ministry of Public Security, drawing on GDPR Article 35 and PIPA Article 28-2, but simplified to suit Vietnam's administrative capacity. Rather than applying universally, DPIA/AIA requirements should be limited to high-risk uses, including facial recognition, biometric identification, behavioural analytics, and anomaly detection in public spaces.

Alongside impact assessments, short-term reforms should establish minimum transparency standards. Public agencies deploying AI surveillance should be required to publish basic information on the purpose of deployment, categories of data collected, retention periods, and responsible authorities. These measures are institutionally feasible because they can be implemented through ministerial circulars or inter-ministerial guidance, without requiring new legislation or the creation of independent bodies.

From a political perspective, this phase is highly feasible. It does not challenge existing power structures, does not require constitutional change, and aligns with Vietnam's ongoing digital-government and administrative-reform agendas. Importantly, it allows policymakers to test governance tools in practice, generating institutional learning before deeper reforms are pursued.

Medium-Term Measures (3–5 years): Establishing a Supervisory Authority and Harmonising Existing Laws

In the medium term, the central reform priority is to address the oversight and enforcement gap identified in RQ2 by establishing a functionally independent Data Protection Authority (DPA) or equivalent supervisory body. Drawing on lessons from GDPR's DPAs and Korea's PIPC, Vietnam does not need to replicate a European-style model; instead, it can establish a specialised authority embedded within an existing ministry but endowed with statutory autonomy in investigations, audits, and enforcement.

This authority should be empowered to: (i) review DPIA/AIA submissions for high-risk AI systems; (ii) audit biometric and AI surveillance deployments; (iii) issue corrective orders or suspension decisions; (iv) receive and resolve complaints from individuals; and

(v) publish annual reports on AI and data-protection governance.

Parallel to institutional reform, Vietnam should undertake harmonisation of existing statutes, including the Law on Cybersecurity (2018), the Law on Cyberinformation Security (2015), and Decree 13/2023/NĐ-CP. The objective is not

wholesale revision, but alignment around core principles: explicit lawful bases for biometric surveillance, clearer purpose limitation, defined retention rules, and procedural safeguards for automated decision-making.

Politically and institutionally, this phase is moderately challenging but feasible. Vietnam has prior experience in establishing specialised regulatory bodies in areas such as competition and anti-corruption. Embedding the DPA within an existing administrative structure—while guaranteeing functional independence—reduces political resistance and institutional disruption. Harmonisation of laws can be framed as technical refinement rather than ideological reform, increasing acceptability.

Long-Term Measures (5–10 years): Enacting a Comprehensive Personal Data Protection Act

In the long term, Vietnam should aim to consolidate its fragmented privacy framework into a comprehensive Personal Data Protection Act. This statute would replace the current patchwork of constitutional provisions, civil-code rules, sectoral laws, and decrees with a unified legal framework governing personal data and AI-enabled processing across all sectors.

Such an Act should explicitly incorporate: (i) ICCPR Article 17 standards of legality, legitimate aim, necessity, and proportionality; (ii) differentiated rules for high-risk AI systems, including biometric and behavioural surveillance; (iii) statutory recognition of the supervisory authority and its powers; (iv) rights of individuals to access, challenge, and seek remedies for automated decisions; and (v) clear coordination mechanisms between data protection, cybersecurity, and national-security laws.

From a political and institutional standpoint, this phase requires the greatest commitment and consensus. However, by the time Vietnam reaches this stage, earlier reforms would have already normalised DPIA/AIA practices, established supervisory capacity, and aligned sectoral laws. This gradual sequencing reduces reform shock and increases the likelihood of sustainable implementation. Moreover, a comprehensive Act would support Vietnam's international integration, enhance trust in digital governance, and strengthen compliance with international human rights obligations.

Taken together, the phased approach outlined above reflects a balance between normative ambition and institutional realism. Short-term measures prioritise practical governance tools; medium-term reforms establish enforceable oversight; and long-term legislation consolidates gains into a coherent legal architecture. This sequencing ensures that privacy protection and human security are strengthened progressively, without undermining Vietnam's digital-transformation goals or governance stability.

By adopting this pathway, Vietnam can move from reactive regulation toward anticipatory, rights-based AI governance, closing the legal and institutional gaps identified in RQ2 and responding effectively to the comparative lessons drawn from GDPR and PIPA in RQ3.

Conclusion

This study has examined the governance of AI-enabled surveillance in Vietnam through the combined lenses of human security and international human rights law, with particular reference to Article 17 of the ICCPR. By integrating doctrinal analysis, comparative insights, and institutional assessment, the article addresses three interrelated research questions concerning privacy risks, legal adequacy, and regulatory reform pathways.

First, the analysis under RQ1 demonstrates that AI-enabled surveillance in Vietnam generates systemic and cumulative risks to privacy that extend beyond technical data-protection concerns. These risks manifest through informational opacity, behavioural chilling, algorithmic bias, and institutional accountability deficits, collectively undermining individual autonomy, dignity, and freedom from fear. Viewed through the human-security framework, privacy emerges not merely as an abstract legal entitlement, but as a condition for meaningful civic participation and personal security in a digitally mediated society.

Second, the assessment under RQ2 reveals that Vietnam's current legal framework remains insufficient to regulate AI-driven surveillance in line with ICCPR standards. While privacy is formally recognised in the Constitution, the Civil Code, and sectoral legislation, significant gaps persist in legality, legitimate aim specification, necessity and proportionality review, as well as in independent oversight and access to remedies. The absence of clear lawful bases for biometric surveillance, the lack of structured impact assessments, and fragmented institutional responsibility expose individuals to the risk of arbitrary or disproportionate interference with their private life.

Third, the comparative analysis under RQ3 shows that the EU's GDPR and South Korea's PIPA offer valuable lessons not because of their complexity, but because of the institutional machinery that renders privacy protections enforceable in practice. Independent supervisory authorities, structured necessity–proportionality assessments, and mechanisms for algorithmic accountability transform legal principles into operational safeguards. Importantly, the study demonstrates that these elements are not unique to Western or highly liberal legal systems; rather, they can be adapted in a context-sensitive manner to countries with strong state coordination and ambitious digital-government agendas, such as Vietnam.

Based on these findings, the article proposes a phased and feasible reform pathway for Vietnam, moving from short-term sectoral guidance and impact-assessment pilots, to medium-term establishment of a functionally independent supervisory authority and legal harmonisation, and ultimately toward a comprehensive Personal Data Protection Act. This incremental approach reflects Vietnam's legal culture and administrative capacity, avoiding abrupt institutional disruption while progressively strengthening rights protection and human security.

The contribution of this study is threefold. Conceptually, it advances the application of human-security theory to AI surveillance governance in a developing-country context. Doctrinally, it provides one of the first systematic ICCPR-based assessments of Vietnam's AI surveillance framework. Practically, it offers a realistic regulatory roadmap grounded in comparative experience and institutional feasibility. Together, these contributions underscore that effective governance of AI surveillance requires not only legal recognition of privacy, but also enforceable institutional arrangements capable of balancing technological innovation, national-security objectives, and the protection of human dignity in the digital age.

References

Aloisit, A., & Gramanott, E. (2019). Artificial intelligence is watching you at work: Digital monitoring, employee monitoring and legal issues in the EU context. *Artificial Intelligence Is Watching You*, *41*(1), 95–122. https://goo.gl/Cv4EAi.

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding Regulation: Theory, Strategy, and Practice*. Oxford University Press.

Bennett, C. J., & Raab, C. D. (2017). The governance of privacy: Policy instruments in

global perspective. In *The Governance of Privacy: Policy Instruments in Global Perspective*. MIT Press. https://doi.org/10.4324/9781315199269

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, *81*, 1–15.

Celeste, E. (2019). Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers and Technology*, *33*(1), 76–99. https://doi.org/10.1080/13600869.2019.1562604

Duberry, J. (2022). Artificial Intelligence and Democracy: Risks and Promises of AI-Mediated Citizen-Government Relations. In *Artificial Intelligence and Democracy: Risks and Promises of AI-Mediated Citizen-Government Relations* (pp. 1–244). Edward Elgar Publishing. https://doi.org/10.4337/9781788977319

Dunleavy, P., & Margetts, H. (2025). Data science, artificial intelligence and the third wave of digital era governance. *Public Policy and Administration*, *40*(2), 185–214. https://doi.org/10.1177/09520767231198737

Ergashev, A. (2023). Privacy Concerns and Data Protection in An Era of AI Surveillance Technologies. *International Journal Of Law And Criminology*, *3*(08), 71–76. https://inlibrary.uz/index.php/ijlc/article/view/38845%0Ahttps://doi.org/10.37547/ijlc/Volume03Issue08-14

Ezzeddine, Y., Bayerl, P. S., & Gibson, H. (2023). Safety, privacy, or both: evaluating citizens' perspectives around artificial intelligence use by police forces. *Policing and Society*, *33*(7). https://doi.org/10.1080/10439463.2023.2211813

Ghosh, A., Saini, A., & Barad, H. (2025). Artificial intelligence in governance: recent trends, risks, challenges, innovative frameworks and future directions. *AI and Society*, *40*(7), 5685–5707. https://doi.org/10.1007/s00146-025-02312-y

Haney, B. S. (2019). Applied Artificial Intelligence in Modern Warfare & National Security Policy. *SSRN Electronic Journal*, *11*, 61. https://doi.org/10.2139/ssrn.3454204

Johari, A., & Sparviero, S. (2025). Privacy and AI: Mitigating the Risks, Leveraging the Opportunities. *Journal. Kommunikation-Medien*, *2025*(17), 1–17.

Kim, D. H., & Park, D. H. (2024). Automated decision-making in South Korea: a critical review of the revised Personal Information Protection Act. *Humanities and Social Sciences Communications*, *11*(1), 1–11. https://doi.org/10.1057/s41599-024-03470-y

Lâm, T. T. (2024). Children's personal information and personal data protection under the laws of the EU, US and Vietnam. *Journal of Infrastructure, Policy and Development*, *8*(14), 8143. https://doi.org/10.24294/jipd8143

Lebovits, H. (2019). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. In *Public Integrity* (Vol. 21, Issue 4). St. Martin's Press. https://doi.org/10.1080/10999922.2018.1511671

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the general data protection regulation. *International Data Privacy Law*, *7*(4), 243–265. https://doi.org/10.1093/idpl/ipx019

National Security Commission on Artificial Intelligence. (2021). National Security Commission on Artificial Intelligence. *Final Report - National Security Commission on Artificial Intelligence*, *February*, 1–756.

Nguyen, T. H. (2024). Investigating Driving Factors of Digital Transformation in the Vietnam Shipping Companies: Applied for TOE Framework. *SAGE Open*, *14*(4), 21582440241301210. https://doi.org/10.1177/21582440241301210

Reddy, M. S., Vamsi, C., & Kathambari, P. (2024). Rescue me : AI Emergency Response and Disaster Management System. *2nd International Conference on Artificial Intelligence and Machine Learning Applications: Healthcare and Internet of Things, AIMLA 2024*, 1–5. https://doi.org/10.1109/AIMLA59606.2024.10531386

Richards, N. M., & Hartzog, W. (2015). Taking Trust Seriously in Privacy Law. *SSRN Electronic Journal*, *19*, 431. https://doi.org/10.2139/ssrn.2655719

Sakpal, S. S. (2024). AI Assisted Real Time Response Systems for National Emergency Preparedness and Disaster Management. *2024 Global Conference on Communications and Information Technologies, GCCIT 2024*, 1–7. https://doi.org/10.1109/GCCIT63234.2024.10862886

Singh, T. (2024). AI-Driven Surveillance Technologies and Human Rights: Balancing Security and Privacy. *Smart Innovation, Systems and Technologies*, *392 SIST*, 703–717. https://doi.org/10.1007/978-981-97-3690-4_53

Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, *40*(2), 137–157. https://doi.org/10.1080/14494035.2021.1928377

Thanh, N. N. (2024). The opportunities and challenges of public policy communication in the context of digital transformation in Vietnam. *Journal of State Management* , *31*(12), 13–21. https://jsm.quanlynhanuoc.vn/jsm/article/view/18

UNDP. (1994). Human Development Report 1994: New Dimensions of Human Security. New York: Oxford University Press. *New York. Retrieved December*, *12*, 2022.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation and Governance*, *12*(4), 505–523. https://doi.org/10.1111/rego.12158

Zuboff, S. (2023). The Age of Surveillance Capitalism. In *Social Theory Re-Wired* (pp. 203–213). Routledge. https://doi.org/10.4324/9781003320609-27