CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

© ***Cadernos de Dereito Actual*** Nº 30. Núm. Ordinario (2025), pp. 102-129

·ISSN 2340-860X - ·ISSNe 2386-5229

Special investigative measures and the right to privacy in Vietnam: A comparative analysis with European human rights standards

Thuyen Duy Trinh[1,*]
University of Economics Ho Chi Minh City

---

[1] Assoc. prof, College of Economics, Law and Government, University of Economics Ho Chi Minh City, Vietnam. Formerly served as an investigator in the police force and a lecturer at the People's Police University. Currently a faculty member at the University of Economics, Law and Government–UEH, with extensive experience in legal research and criminal investigation. https://orcid.org/0009-0008-1093-1382; E-mail: thuyentd@ueh.edu.vn (corresponding author).

Abstract: From a comparative legal perspective, the regulation of special investigative measures in Vietnam reveals both progress and paradox. The codification of covert techniques such as surveillance, interception, and data collection has transformed informal police discretion into a framework of procedural legality. Yet, this evolution remains largely internal to state institutions and insufficiently aligned with the external safeguards of human rights law. The Vietnamese system relies on prosecutorial authorization, lacks judicial pre-approval, and omits a proportionality test that would balance state necessity against individual privacy. By contrast, European jurisprudence, grounded in Articles 8 of the European Convention on Human Rights and 17 of the ICCPR, regards legality, necessity, proportionality, and independent oversight as indispensable to the rule of law. The absence of these principles in Vietnam's practice marks a conceptual gap between codified control and accountable power. A normative recalibration is therefore required one that constitutionalizes limits on investigative authority, embeds judicial review, and restores proportionality as the moral center of criminal procedure.

Keywords: Special Investigative Measures, Privacy Rights, Judicial Oversight, Human Rights

1. Introduction

Since the end of World War II, human rights theory and law have been constructed upon the foundational principles of human dignity, liberty, and equality, with a pivotal turning point marked by the adoption of the Universal Declaration of Human Rights in 1948 (UDHR)[2] and the twin international covenants of 1966 the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR).[3,4] Within legal scholarship, numerous jurists have affirmed that human rights serve not only as safeguards against arbitrary interference but also as normative frameworks for the creation of an "autonomous space" in which individuals may form and pursue their own choices[5,6,7,8]. In the informational dimension, the works of Daniel Solove, Mireille Hildebrandt, and Roger Brownsword emphasize that modern privacy is no longer confined to the notion of "the right to be let alone"[9,10,11], but rather encompasses the capacity to control the lifecycle of personal data from its collection and storage to its use and dissemination. This reconceptualization reflects a shift from static notions of privacy toward dynamic models of informational self-determination in the digital age.

---

[2] ASSEMBLY, U. G. (1948). "Universal declaration of human rights". UN General Assembly, 302(2), 14-25.
[3] RESOLUTION, G. A. (1966). "International covenant on economic, social and cultural rights". General Assembly Resolution A.
[4] GENERAL ASSEMBLY RESOLUTION. The International Covenant on Civil and Political Rights [online]. 1966. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (accessed on 26 October 2025).
[5] HILDEBRANDT, M. "Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology". In Smart Technologies and the End (s) of Law: Edward Elgar EBooks, 2016.
[6] BROWNSWORD, R. "Law, Technology and Society: Reimagining the Regulatory Environment". (1st ed.) Edtion ed.: Routledge, 2019.
[7] SOLOVE, D. J. (2002). "Conceptualizing Privacy". California Law Review, 90(4), 1087-1155.
[8] WARREN, S. D., BRANDEIS, L. D. (1890). "The Right to Privacy". Harvard Law Review, 4(5).
[9] HILDEBRANDT M. 2015. Ibid.
[10] BROWNSWORD, R. 2019. Ibid.
[11] WARREN, S. D., (1890). Ibid.

Nowadays, the evolution of modern criminal justice increasingly relies on the deployment of special investigative measures such as electronic surveillance, interception of communications, undercover operations, and data collection to combat organized crime, terrorism, corruption, and drug-related offenses. These techniques have become institutionalized within law enforcement systems worldwide. However, their proliferation raises a profound normative dilemma: how can the State safeguard collective security while simultaneously respecting the fundamental rights that constitute the foundation of democratic legitimacy? From a human rights perspective, this dilemma converges most sharply on the *right to privacy* and the *protection of personal data* rights recognized as essential to human dignity, autonomy, and the free development of personality. These protections are enshrined in international legal instruments such as *Article 17 of the ICCPR)* and *Article 8 of the European Convention on Human Rights (ECHR)*. As Singh and Sweksha emphasize, privacy safeguards are indispensable for ensuring due process and preventing arbitrary state interference, particularly in the context of intrusive surveillance and data collection.[12] Similarly, Prysiazhniuk underscores the tension between the use of digital evidence in criminal proceedings and the imperative to uphold privacy rights under international standards.[13] Komukai further highlights the risks posed by third-party data transfers during investigations, advocating for stricter legal constraints and transparency obligations.[14]

Within the European legal order, these conditions have been further elaborated by the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), creating a sophisticated framework for assessing state surveillance and covert investigative techniques. The ECtHR's jurisprudence under Articles 8 and 10 ECHR requires that any interference with private life or correspondence be *in accordance with the law*, pursue a *legitimate aim*, and be *necessary in a democratic society*[15,16]. This tripartite test has evolved into a robust standard of proportionality, demanding clear statutory authorization, independent judicial oversight, and effective safeguards against abuse. Parallel to this, the CJEU interpreting the EU Charter of Fundamental Rights, particularly Articles 7 and 8 has reinforced the same triad through the principles of lawfulness, purpose limitation, data minimization, and proportionality as codified in the General Data Protection Regulation (GDPR)[17] and Directive (EU) 2016/680 on data processing for law enforcement[18]. In cases such as *Digital Rights Ireland* (2014),[19] *Tele2 Sverige*

---

[12] PRIYANKA, S. AND SWEKSHA. (2024). "Role of Right to Privacy in the Criminal Justice System". International Journal for Multidisciplinary Research, 6(3), 1-16.

[13] PRYSIAZHNIUK, I. (2023). "Use of Digital Evidence in Criminal Process: Some Issues of Right to Privacy Protection". Visegrad Journal on Human Rights, 5, 81-88.

[14] KOMUKAI, T. "Privacy Protection During Criminal Investigations of Personal Data Held by Third Parties". In IFIP International Conference on Human Choice and Computers. Cham: Springer International Publishing, 2022, p. 200-212.

[15] EUROPE, C. O. European Convention on Human Rights, [online]. 1950. Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG (accessed on 26 October 2025).

[16] EUROPEAN COURT OF HUMAN RIGHTS. (2025). "Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life". ECHR Knowledge Sharing (ECHR-KS).

[17] GENERAL DATA PROTECTION REGULATION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC In., 2016. EUROPE, C. O. European Convention on Human Rights, [online]. 1950. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 26 October 2025).

[18] DIRECTIVE (EU). Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free

(2016),[20] and *La Quadrature du Net* (2020)[21], the CJEU held that indiscriminate or bulk data retention regimes violated these principles because they lacked specific targeting, temporal limitation, and independent authorization. Together, the ECtHR and CJEU jurisprudence form the European benchmark for balancing security imperatives with the right to privacy, establishing that covert investigation must always remain the exception, not the norm. This European framework has global significance. It demonstrates that effective criminal investigation can coexist with strict human rights guarantees if states institutionalize transparency, accountability, and proportionality. The challenge lies not in the existence of special measures themselves but in the absence of legal architecture that defines their boundaries and ensures oversight. The ECtHR's warning in Roman Zakharov v. Russia[22] that a system of secret surveillance may "undermine or even destroy democracy under the cloak of defending it" captures the essence of this paradox. Such reasoning resonates far beyond Europe, providing valuable guidance for jurisdictions that are currently reforming their criminal procedure laws to align with international human rights standards.

In the Vietnamese context, the issue has acquired renewed relevance following the adoption of the Criminal Procedure Code 2015, amended in 2021, 2025(CPC),[23] which officially recognizes certain *special investigative measures* such as the interception of communications, controlled deliveries, and the use of technical surveillance devices. These provisions, inspired in part by comparative models, aim to enhance the effectiveness of criminal investigations against serious offences, particularly organized and high-tech crimes. However, the legal framework remains in an early stage of development, and several questions persist concerning its compatibility with constitutional rights and international obligations. Article 21 of the 2013 Constitution of Vietnam affirms that "everyone has the right to inviolability of private life, personal secrets and family secrets; information about private life, personal secrets, and family secrets shall be safely protected by law." Yet, the practical implementation of these rights in the context of criminal investigations is still uncertain. The CPC lacks detailed provisions on judicial authorization, time limits, data retention, and ex post supervision, leaving substantial discretion to investigative bodies. Consequently, while the law grants investigative efficiency, it also raises legitimate concerns about potential overreach and insufficient safeguards for personal data and communication privacy. This research therefore

---

movement of such data, and repealing Council Framework Decision 2008/977/JHA. In., 2016. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680 (accessed on 26 October 2025).

[19] COURT OF JUSTICE OF THE EUROPEAN UNION. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources (Joined Cases C-293/12 and C-594/12). EUR-Lex. In., 2014. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293 (accessed on 26 October 2025).

[20] COURT OF JUSTICE OF THE EUROPEAN UNION. Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others (Joined Cases C-203/15 and C-698/15). EUR-Lex / CURIA. In., 2016. Available at: https://curia.europa.eu/juris/liste.jsf?num=c-203/15 (accessed on 26 October 2025).

[21] COURT OF JUSTICE OF THE EUROPEAN UNION. La Quadrature du Net and Others v. France (Joined Cases C-511/18, C-512/18, and C-520/18). In., 2020. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CA0511 (accessed on 26 October 2025).

[22] EUROPEAN COURT OF HUMAN RIGHTS. Roman Zakharov v. Russia (Application no. 47143/06). Strasbourg: ECtHR.HUDOC. In., 2015. Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22] (accessed on 26 October 2025).

[23] NATIONAL ASSEMBLY. Criminal Procedure Code. In., 2015. Available at: https://thuvienphapluat.vn/van-ban/Thu-tuc-To-tung/Van-ban-hop-nhat-46-VBHN-VPQH-2025-Bo-Luat-To-tung-hinh-su-647146.aspx (accessed on 26 October 2025).

proceeds from a central premise: that the assessment of *special investigative measures* must be grounded in human rights law, with particular emphasis on the right to privacy and data protection. By examining the European Union's legal standards and comparing them with Vietnam's existing framework, the study seeks to clarify the normative requirements for lawful, legitimate, and necessary use of investigative powers. The inquiry ultimately aims to identify how Vietnam can reconcile its pursuit of security and justice with the preservation of fundamental freedoms a balance that defines not only the rule of law, but the very meaning of democracy in contemporary criminal justice.

In the context of evolving digital surveillance, Vietnam's use of the SIMs raises important questions about the balance between state security and individual privacy. This paper explores two key research questions:

How well does Vietnam's Criminal Procedure Code align with international human rights standards on special investigative measures, particularly concerning privacy rights and data protection?

What are the gaps in Vietnam's legal framework in comparison to European human rights jurisprudence, and how can they be addressed to enhance judicial oversight and protect individual privacy?

2. Methodology

In Vietnam (due to political and legal characteristics), Special Investigative Measures (SIMs), when applied in investigative activities, are confidential and not disclosed during trial proceedings. Consequently, the author faces considerable difficulties in accessing case files and collecting data from state agencies. Therefore, quantitative methods based on publicly available data are not feasible in the Vietnamese context. This study employs several specific methods as follows:

2.1. Materials and sources

The primary materials consist of Vietnam's CPC provisions governing SIMs (Chapter XVI, Arts. 223–228) and related domestic instruments on privacy and data protection. The comparative materials include international human rights norms primarily Article 8 ECHR and Article 17 ICCPR and authoritative jurisprudence and guidance that specify minimum safeguards for secret surveillance. Secondary materials include peer-reviewed scholarship, judicial guidance, and expert commentary by Vietnamese and international authors relevant to SIMs oversight, proportionality, data governance, and remedies.

2.2. Doctrinal and comparative legal analysis

The first component applies doctrinal and comparative legal analysis to interpret the relevant provisions of the CPC and related instruments, comparing them with international human rights frameworks such as Article 8 of the ECHR and Article 17 of the ICCPR. This method aims to identify the strengths and weaknesses of Vietnam's current provisions on the SIMs, highlighting gaps in legality, necessity, and proportionality within the regulatory framework.Specifically, the comparative legal analysis will:

Identify conceptual and procedural gaps in the application of SIMs in Vietnam, particularly regarding the lack of legal principles such as independent oversight and the lack of proportionality and necessity tests for investigative measures.

Assess the practical impact of these shortcomings on the protection of defendants' rights, particularly privacy and data protection rights, within the criminal procedure system.

Propose interpretive approaches to improve transparency, accountability, and human rights compliance in the application of SIMs in Vietnam, aligned with international standards on privacy rights and data protection.

2.3. Qualitative interpretive method

The second, component adopts a qualitative interpretive method based on a synthesis of academic commentary, judicial guidelines, and expert opinions from Vietnamese and international scholars. These sources provide indirect but credible evidence of systemic vulnerabilities, particularly the concentration of approval power within the Procuracy and the absence of judicial or civilian supervision. By treating these expert perspectives as interpretive data, the research constructs a plausible account of how secrecy, institutional hierarchy, and limited transparency interact to create accountability deficits. At the same time, this method also conducts analysis of the provisions in the CPC, specifically Articles 223-228, to clarify the areas that are ambiguous or lack detail in the application of SIMs. The use of international standards helps propose improvement solutions, such as requiring independent oversight, post-application notification rights for SIMs, and privacy protection measures during criminal proceedings. The aim is not only to analyze the theory but also to develop practical solutions, ensuring that special investigative measures are implemented transparently, responsibly, and with full protection of human rights.

2.4. Limitations

Because the study relies on publicly available sources, it does not make factual claims about specific classified operations. Its conclusions are normative and structural: they assess the safeguard density and institutional independence of the legal framework and propose reforms that are legally justified and institutionally plausible within Vietnam's criminal justice system.

3. Content

3.1. Defining special investigative measures: Legal nature, theoretical controversies, and human rights implications

The concept of the SIMs is best understood as a category of covert procedural techniques used in serious criminal investigations when ordinary methods are insufficient. What distinguishes SIMs is not simply secrecy, but the combination of heightened intrusiveness and exceptional procedural capacity, which demands correspondingly stronger legal safeguards and oversight within a rule-of-law framework.[24,25] Yet the more the law resorts to secrecy, the more it exposes its own fragility: it must ensure that exceptional powers remain constitutionally bounded and morally justified.

I believe that any attempt to define SIMs must start from this dialectic tension between security and liberty. Scholars like Kruisbergen et al and Dahl argue that covert operations are not simply pragmatic tools but essential responses to the increasing invisibility of organized crime.[26,27] Dahl even conceptualizes surveillance as a form of "chameleonizing," suggesting that investigators must blend into their

[24] VERVAELE, J. A. (2009). "Special procedural measures and the protection of human rights General report". Utrecht Law Review, 5(2).
[25] KRUISBERGEN, E. W., D. DE JONG AND E. R. KLEEMANS. (2011). "Undercover Policing: Assumptions and Empirical Evidence". The British Journal of Criminology, 51(2), 394-412.
[26] DAHL, J. Y. (2022). "Chameleonizing: A microsociological study of covert physical surveillance". European Journal of Criminology, 19(2), 220-236.
[27] KRUISBERGEN, E. W., 2011. Ibid.

environment to observe criminal activity undetected. This view often described as functionalist frames SIMs as a necessary adaptation of the justice system to modern criminal threats. In this sense, necessity becomes both the justification and the definition of special investigation. However, I find this reasoning normatively troubling. A workable definition of SIMs must therefore start from their functional effect on protected interests: they are designed to obtain information while the affected person is unaware, which reduces the possibility of contemporaneous challenge and increases the risk of normalization of extraordinary powers. The central legal concern is not moral abstraction, but whether the use of covert techniques can remain legitimate when it creates structural asymmetries between the state and the individual and may blur the boundary between detection and induced wrongdoing.[28]

Within Vietnamese jurisprudence, this definitional issue has likewise been examined, but predominantly from an institutional and procedural perspective. Pham Quang Phuc equates SIMs with *special reconnaissance measures* used by the police, emphasizing that their defining characteristic lies in secrecy itself "biện pháp trinh sát có tính chất đặc thù, rõ nét nhất đó là tính chất bí mật."[29] Phan Van Chanh refines the scope, arguing that SIMs are investigative activities conducted by specialized agencies within the People's Public Security and People's Army after the initiation of criminal proceedings, designed to identify offenders through secret methods codified in the Criminal Procedure Code.[30] Le Huynh Tan Duy shares this approach but stresses their evidentiary purpose: these measures "aim to collect evidence proving the crime, the perpetrator, and other relevant circumstances for resolving the case."[31] Nguyen Son Phuoc goes further by synthesizing these views into a more comprehensive definition SIMs are investigative methods prescribed by law, performed secretly after the initiation of proceedings, applicable only to particularly serious offences, and aimed at collecting materials and evidence for case resolution.[32] These definitions are undeniably valuable, for they anchor SIMs within the procedural architecture of Vietnamese criminal law. They delineate the competent authorities, the procedural stage, and the evidentiary objective all crucial elements for legal certainty. Yet, I believe that they remain primarily institutional rather than normative. They explain *who* may conduct these measures and *when*, but not *why* such extraordinary powers can be justified in a constitutional democracy. This is the conceptual gap between domestic proceduralism and the international discourse on human rights.

From my perspective, the functionalist definition must therefore be balanced by what may be called the rule-of-law constraint. Esen reminds us that any interception of communication under *Article 8 of the ECHR*must be "in accordance

---

[28] HILL, D. J., S. K. MCLEOD AND A. TANYI. (2024). "Policing, undercover policing and 'dirty hands': the case of state entrapment". Philosophical Studies, 181(4), 689-714.

[29] TUYEN, P. M. (2019). "Reflections on Special Investigative Procedures under the 2015 Criminal Procedure Code". Procuratorate Studies, 06. Available at: https://vjol.info.vn/index.php/tks/article/download/46430/37679/ (accessed on 26 October 2025).

[30] CHANH, P. V. (2018). "Special investigative procedural measures in Vietnam's criminal proceedings". Journal of People's Procuracy of Vietnam, 11. Available at: https://tlpl.moj.gov.vn/Pages/chi-tiet-bai-trich.aspx?ItemID=1506&CategoryBTTC=BTTC (accessed on 26 October 2025).

[31] DUY, L. H. T. (2023). "Comparative research on special investigation measures and experiences for Vietnam". Procuratorate Studies, 03. Available at: https://vjol.info.vn/index.php/tks/article/view/82153 (accessed on 26 October 2025).

[32] PHUOC, N. S. (2022). "Assessment of provisions on special investigative measures in the 2015 criminal procedure code and recommendation for complete". Journal of Science and Technology, 5(3). Available at: https://doi.org/10.56097/binhduonguniversityjournalofscienceandtechnology.v5i3.56 (accessed on 26 May 2025).

with the law," meaning that it must be accessible, foreseeable, and subject to effective supervision.[33] This is not merely a technical requirement but a constitutional safeguard. The ECHR, in its landmark cases *Klass v. Germany*[34] and *Zakharov v. Russia,*[35] established that covert surveillance can only be justified when it passes three cumulative tests: legality, necessity, and proportionality. These principles transform SIMs from acts of discretion into acts of constitutional responsibility. I hold that this legalist understanding offers a more legitimate foundation: it does not deny the need for special measures but insists that their "specialness" lies precisely in the intensity of legal control required. As Vervaele elaborates, such measures are "lawful deviations" that remain valid only within the orbit of constitutional oversight.[36]

Still, the law's emphasis on authorization may conceal a deeper sociological reality. Loftus and Goold vividly describes covert surveillance as part of "the invisibilities of policing," a phrase that captures both the power and the danger of modern investigative practices.[37] Surveillance is not only a legal act but a social experience; it shapes the psychology of citizenship. Stevens et al through their fieldwork in Uganda and Zimbabwe, found that even the *possibility* of surveillance produces "chilling effects" citizens begin to censor themselves, avoid political assembly, and internalize fear.[38] Similarly, Matar and Murray warns that international human rights law must evolve to defend the *integrity of personal identity*, not just isolated rights, against the pervasive logic of surveillance.[39] I find this dimension particularly compelling because it reframes SIMs not as neutral instruments but as *social practices that reconfigure the relationship between state and individual*. When people adapt their behavior to perceived observation, the right to privacy is not only violated it is psychologically surrendered. It is troubling that the law often measures harm only in terms of concrete intrusion, ignoring these subtle, invisible effects on human autonomy.

Legal systems that permit undercover operations also face the moral question of entrapment whether the state may justly provoke the commission of crime in order to detect it. Ormerod, Ho both reject a purely pragmatic view, insisting that when the state manufactures the offense, it ceases to enforce justice and begins to impersonate criminality.[40,41] Taylor further warns that in such circumstances, "the process itself becomes contaminated."[42] I concur with these critiques. When investigative authorities deliberately induce unlawful behavior, the legitimacy of

---

[33] ESEN, R. (2012). "Intercepting Communications 'In Accordance with the Law'". The Journal of Criminal Law, 76(2), 164-178.

[34] EUROPEAN COURT OF HUMAN RIGHTS. Case of Klass and others v. Germany (Application no. 029/71).HUDOC. In.: European Court Of Human Rights, 1978. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]} (accessed on 26 May 2025).

[35] EUROPEAN COURT OF HUMAN RIGHTS. 2015. Ibid.

[36] VERVAELE, J. A. 2009. Ibid.

[37] LOFTUS, B. AND B. GOOLD. (2012). "Covert surveillance and the invisibilities of policing". Criminology & Criminal Justice, 12(3), 275-288.

[38] STEVENS, A., FUSSEY P., MURRAY, D., HOVE, K., SAKI, O. (2023). "'I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe". Big Data & Society, 10(1), 20539517231158631.

[39] MATAR, R. AND D. MURRAY. (2025). "Re-thinking international human rights law's approach to identity in light of surveillance and AI". Human Rights Law Review, 25(3), ngaf016.

[40] HO, H. L. (2011). "State entrapment". Legal Studies, 31(1), 71-95.

[41] ORMEROD, D. AND A. ROBERTS. (2002). "The Trouble with Teixeira: Developing a Principled Approach to Entrapment". The International Journal of Evidence & Proof, 6(1), 38-61.

[42] TAYLOR, C. (2005). "Entrapment: Abuse of Process:R v Lewis (Michael William) [2005] EWCA Crim 859". The Journal of Criminal Law, 69(5), 380-384.

prosecution collapses regardless of the outcome. Murphy's analysis of the Canadian *Mr Big* technique exposes this vividly: simulated criminal organizations elicited confessions through deception and psychological coercion, leading courts to exclude the evidence as a violation of the right to silence[43] . Personally, I see in these cases a fundamental truth the boundary between discovery and creation of crime is not procedural but moral. A state that invents guilt in order to prove it betrays the essence of the rule of law.

Defining SIMs is less about listing techniques than about confronting the boundary between legitimate coercion and illegitimate manipulation. A human-rights-centered definition views SIMs as legally authorized, covert, and intrusive tools, justified only when necessary, proportionate, and subject to effective oversight. The burden of justification lies with the state, while privacy under Article 17 of the ICCPR affirms informational autonomy. As technology advances through algorithmic surveillance, data mining, and predictive policing the definition must adapt. Bulk interception, as Turanjanin warns, undermines individualized suspicion and risks turning every citizen into a potential suspect.[44]

Building on this definitional concern, my study of human rights and criminal justice, I argue that the urgent task is not to define investigative tools but to secure accountability. Many jurisdictions, including Vietnam, have codified SIMs without independent oversight or notification, risking legality in form but not in substance. Special investigative measures embody a constitutional paradox: they preserve order through instruments that threaten the moral order of law. The challenge is to civilize them embedding transparency, necessity, and proportionality so that what remains unseen is never unaccountable. Defining SIMs thus reflects constitutional maturity and the balance between power and right.[45]

3.2. European human rights standards on privacy and their implications for special investigative measures

The relationship between the right to privacy and SIMs reveals one of the most intricate tensions within modern criminal procedure: the coexistence of secrecy and rights in the same legal system. Privacy, as a human right, serves not merely to protect personal intimacy but to secure the very condition of autonomy from arbitrary power. SIMs, on the other hand, are designed precisely to pierce secrecy in the pursuit of truth. Their intersection, therefore, is not accidental but dialectical each both challenges and defines the limits of the other. I believe that any assessment of the legal regime governing SIMs must begin with the normative architecture of privacy itself, both as recognized under international human-rights law and as institutionalized in Vietnam's domestic legal system.

Under international law, the right to privacy occupies a central position in the moral and constitutional order of democratic states. *Article 17 of the ICCPR*[46] provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence." The *Human Rights Committee*, in *General Comment No. 16 (1988)*, interpreted this provision expansively, holding that even legally authorized interferences could become unlawful if they were arbitrary, unnecessary, or disproportionate.[47] Privacy is therefore not an absolute

---

[43] MURPHY, B. AND J. ANDERSON. (2016). "Confessions to Mr Big:A new rule of evidence?". The International Journal of Evidence & Proof, 20(1), 29-48.
[44] TURANJANIN, V. (2022). "Special investigative measures: Comparison of the Serbian Criminal Procedure Code with the European Court of Human Rights Standards". The International Journal of Evidence & Proof, 26, 34-60.
[45] LOFTUS, B., 2012. Ibid.
[46] GENERAL ASSEMBLY RESOLUTION. 1966. Ibid.
[47] THE HUMAN RIGHTS COMMITTEE. CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection

shield but a conditional right, one that allows for interference only when justified by compelling public interest under strict legal controls. Similarly, *Article 8 of the ECHR* enshrines the "right to respect for private and family life, home and correspondence,"[48] and prohibits interference unless "in accordance with the law" and "necessary in a democratic society." These two provisions ICCPR Article 17 and ECHR Article 8 form the dual foundation upon which most modern legal systems, including Vietnam's, conceptualize privacy.

The underlying rationale of this model is that the exercise of investigative power, if left unchecked, poses a latent risk to democratic governance itself. Surveillance, by its very nature, intrudes upon the sphere of privacy in which citizens develop their autonomy, opinions, and capacity for political participation. Even when justified by national security or crime prevention objectives, intrusive measures may generate indirect social harm, such as deterrence of free expression and erosion of public trust in institutions. These consequences, sometimes referred to as *chilling effects*, highlight why legality, foreseeability, and proportionality are indispensable elements of human rights analysis. Yet the ECtHR does not assess such effects abstractly; rather, it examines whether domestic laws and practices embody concrete legal safeguards sufficient to prevent abuse and to ensure accountability.

The first criterion *in accordance with the law* constitutes the cornerstone of legality under the ECHR. The Court has repeatedly emphasized that legality, in this context, extends beyond the mere existence of a statutory basis. A law authorizing surveillance must be accessible to the public, formulated with sufficient precision, and provide adequate safeguards against arbitrary interference. In its landmark decision in *Klass and Others v. Germany* (1978), the ECtHR recognized that democratic societies may require secret surveillance to protect national security. However, it insisted that the exercise of such powers must be regulated by clear legal rules that delineate the scope and conditions of use, the categories of persons affected, the duration of monitoring, and the oversight mechanisms ensuring judicial or parliamentary control. The Court declared that the law must indicate "with sufficient clarity the scope and manner of exercise of the discretion conferred on the authorities" to prevent covert interference from degenerating into a tool of political repression (European Court of Human Rights, 1978, para. 50).

This demand for foreseeability was reinforced decades later in *Roman Zakharov v. Russia* (2015), where the Court held that Russia's legal framework for intercepting communications was incompatible with Article 8. Although the relevant statutes formally required authorization, in practice security agencies could directly access telephone networks without individualized warrants or meaningful external control. The Court found that such a system, operating in secrecy and devoid of effective oversight, risked "undermining or even destroying democracy under the cloak of defending it" (European Court of Human Rights, 2015, para. 243). Through these judgments, the ECtHR established that the rule of law in the surveillance context demands not only formal authorization but also substantive transparency and independent control. Citizens must be able to foresee the circumstances in which the state may interfere with their private life and communications; otherwise, the uncertainty itself breeds fear and restraint, which are incompatible with democratic confidence.

The second criterion the pursuit of a *legitimate aim* defines the substantive boundaries within which interference may lawfully occur. Article 8(2) of the Convention lists a closed catalogue of acceptable purposes: national security, public safety, economic well-being of the country, prevention of disorder or crime,

---

of Honour and Reputation. In., 1988. Available at: https://www.refworld.org/legal/general/hrc/1988/en/27539 (accessed on 26 May 2025).

[48] EUROPEAN COURT OF HUMAN RIGHTS. 2025. Ibid.

protection of health or morals, and protection of the rights and freedoms of others. These categories are narrowly construed, and the burden lies on the state to demonstrate that its measure genuinely serves one of these aims. The ECtHR's reasoning in *Leander v. Sweden* (1987) illustrates this principle: while Sweden argued that background security checks pursued the legitimate goal of protecting national security, the Court still examined whether the measure's scope and secrecy were proportionate to that goal. The mere invocation of national security or crime prevention is never sufficient; governments must show that the interference addresses a concrete and pressing need. As the Court warned in *Roman Zakharov*, an overly elastic interpretation of "national security" could render the protection of privacy illusory (European Court of Human Rights, 2015, para. 255).

In parallel, the CJEU applying the Charter of Fundamental Rights of the European Union, has adopted a comparable approach when evaluating data retention and surveillance legislation. In *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12, 2014), the CJEU annulled the EU Data Retention Directive because it required telecommunications providers to store metadata of all users, without differentiation, for up to two years. The Court held that such general and indiscriminate retention "entails an interference with the fundamental rights of practically the entire European population" and therefore exceeded what could be justified by any legitimate aim of combating serious crime. This reasoning was reaffirmed in *Tele2 Sverige AB* (C-203/15, 2016) and *La Quadrature du Net* (C-511/18, 2020), where the CJEU clarified that only targeted, time-limited, and judicially supervised retention could meet the threshold of legitimacy. These rulings demonstrate a convergence between the Strasbourg and Luxembourg courts in insisting that special investigative powers must be linked to specific, narrowly defined objectives rather than broad policy ambitions.

The third and most demanding requirement, that a measure be *necessary in a democratic society*, encapsulates the proportionality principle and the very essence of human rights protection in Europe. Necessity does not imply mere usefulness or convenience for the authorities; it requires proof that the measure corresponds to a "pressing social need" and that no less intrusive alternative could achieve the same aim. In applying this standard, the ECtHR has developed a dense body of criteria concerning safeguards and oversight. In *Weber and Saravia v. Germany* (2006), the Court held that even large-scale interception could, in principle, be compatible with Article 8, provided that the law clearly defined the nature of offences justifying interception, the duration and procedure of authorization, and the mechanisms of subsequent supervision. However, where such safeguards are absent, the Court has not hesitated to find violations. The judgment in *Big Brother Watch and Others v. United Kingdom* (2021) represents a major articulation of these principles: the Court concluded that the UK's bulk interception regime under the Regulation of Investigatory Powers Act lacked prior independent authorization, adequate oversight, and effective redress mechanisms, thereby failing the necessity test. Crucially, the Court tied this procedural deficiency to a substantive democratic concern, warning that unchecked surveillance "has the potential to weaken the confidence of citizens in the functioning of the democratic institutions which it purports to protect" (European Court of Human Rights, 2021, para. 387).

The European Union's own legal instruments reinforce these human rights standards. Article 52(1) of the EU Charter of Fundamental Rights stipulates that any limitation on the exercise of rights must be provided by law, respect the essence of the rights, and be both necessary and proportionate. The General Data Protection Regulation (GDPR) and Directive (EU) 2016/680 on data processing for law enforcement purposes codify these requirements through principles of lawfulness, purpose limitation, data minimization, and independent supervision. Read together, the ECtHR and CJEU jurisprudence, the Charter, and the GDPR establish a

multilayered architecture of accountability that subjects all forms of covert investigation to strict scrutiny.

From a normative perspective, the European model constructs a delicate equilibrium between state security and individual autonomy. The requirement of legality prevents secret laws and unreviewable discretion; the requirement of legitimacy confines surveillance to socially justifiable purposes; and the necessity standard ensures that proportionality and democratic oversight remain central. These cumulative guarantees aim to prevent a shift from targeted investigation to mass surveillance and to preserve the public's trust in the rule of law. As Gerards (2013) observes, the *necessity test* functions not merely as a procedural device but as a substantive inquiry into the compatibility of investigative practices with democratic values such as transparency, accountability, and respect for human dignity.

Since 2018, the European Union's General Data Protection Regulation (GDPR) has extended these human rights principles into a comprehensive legal framework governing the processing of personal data. The GDPR enshrines fundamental principles of lawfulness, fairness, transparency, purpose limitation, data minimization, and storage limitation (Article 5), alongside the right to erasure ("right to be forgotten," Article 17). Of particular importance is Article 23, which allows Member States to restrict data-subject rights for purposes of national security and criminal investigation, but only when such restrictions are necessary, proportionate, and subject to appropriate safeguards. This conditional approach transforms privacy from an absolute right into a structured balance between individual autonomy and collective security.

Complementing the GDPR, the Law Enforcement Directive (Directive (EU) 2016/680) provides a parallel regime specifically for data processing by criminal justice and law enforcement authorities. It requires that any collection or use of personal data for investigative purposes comply with the principles of accuracy, integrity, purpose limitation, and supervision by an independent data protection authority (Article 41). In this way, the Directive operationalizes the ECHR's procedural guarantees within the context of policing and criminal justice, ensuring that investigative necessity does not become a pretext for unchecked intrusion.

The Figure 1 illustrates the four-tiered supervision mechanism required by Directive (EU) 2016/680, ensuring that any special investigative measure is authorized, supervised, reviewed, and data-handled under independent judicial and administrative oversight.

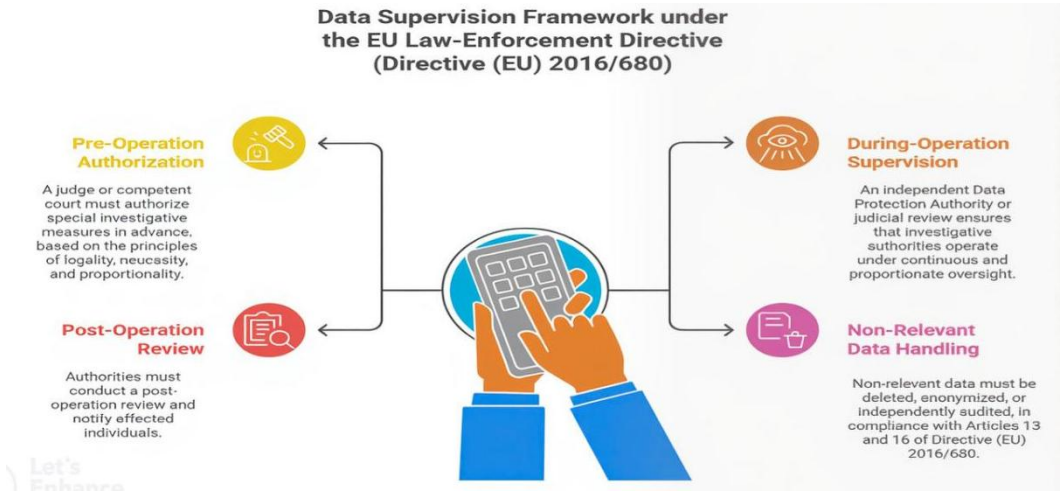

Figure 1. Data supervision framework under the EU law-enforcement directive (directive (EU) 2016/680).

3.3. Legal regulation of special investigative measures in Vietnam: Between secrecy and constitutional rights

In Vietnam, privacy is protected under *Article 21 of the Constitution of 2013*, which provides that "*everyone has the right to the inviolability of private life, personal secrets, and family secrets; the safety of correspondence, telephone, telegram, and other forms of private communication*." This constitutional text is further operationalized by *Article 38 of the 2015 Civil Code* and *Article 159 of the 2015 Criminal Code*, both criminalizing acts of unlawfully collecting, storing, or disclosing private information. However, the right to privacy is not absolute. Article 14(2) of the 2013 Constitution also stipulates that "human rights and citizens' rights may only be restricted by law in cases of necessity for reasons of national defense, national security, social order and safety, social morality, and public health." This provision serves as the legal basis for the inclusion of special investigative measures in the CPC. These measures such as wiretapping, covert surveillance, and data interception are permitted under strict legal conditions and are intended to serve the legitimate aim of preventing and combating serious crimes. By allowing such exceptions, the law seeks to strike a careful balance between the protection of individual privacy and the broader need to ensure public safety and national security. The implementation of these special investigative techniques must adhere to procedural safeguards and judicial oversight to prevent abuse and to uphold the rule of law.

The special investigative measures are stipulated in six specific articles (from Article 223 to Article 228) under Chapter XVI of the CPC, as amended and supplemented in 2021,2025. Article 223 of the 2015 Criminal Procedure Code stipulates three types of special investigative measures: (1) covert audio and video recording; (2) covert telephone interception; and (3) covert collection of electronic data. Specifically, covert audio and video recording refers to the measure whereby competent authorities secretly install, monitor, and operate technical devices (such as cameras, audio recorders, or photographic equipment) to record the voices and capture the images of individuals suspected of committing crimes, as requested by the investigating agency, for the purpose of collecting documents and evidence to ensure objective case resolution. Covert telephone interception is a measure involving the secret intrusion into and recording of conversations and exchanges conducted via telephone by individuals suspected of criminal activity, upon the request of the investigating agency, in order to gather evidentiary materials for case resolution. Covert collection of electronic data refers to the measure by which competent authorities secretly gather information in electronic form, including symbols, text, numbers, images, and audio that are created, stored, or transmitted via electronic means. Such data may be encrypted or deliberately concealed by users, particularly in cases involving high-tech crimes where offenders often employ sophisticated methods to hide information and documents related to their criminal activities. This measure enables investigative bodies to access critical digital evidence that would otherwise remain inaccessible, thereby supporting the objective and effective resolution of criminal cases.

The types of criminal offences subject to the application of *special investigative measures* include crimes against national security, drug-related offences, corruption offences, terrorism, money laundering, and other organized crimes classified as particularly serious. The law specifies these categories of offences as the only circumstances under which special investigative measures may be employed; they may not be applied in all cases. This restriction is designed to prevent abuse or arbitrary expansion of such measures, thereby safeguarding individual liberty and privacy. The offences for which special investigative measures are permitted are those that infringe upon particularly important legal interests of national security offences that may endanger the institutional foundations and leadership of the

Communist Party and the State, and that threaten to undermine the Party's policies and the State's laws on building a socialist rule-of-law system grounded in democracy, justice, and civility. As for crimes of terrorism, corruption, drug trafficking, money laundering, and other forms of organized criminality deemed particularly serious, these offences, in addition to their inherent gravity, are often perpetrated by specialized and organized actors employing sophisticated and audacious methods. Without the application of special investigative measures, such crimes would be extremely difficult to detect, disrupt, and prevent in a timely and effective manner.

3.3.1. Regarding the authority to decide on the application of special investigative measures

Article 225 of the *CPC*, The Heads of provincial-level investigating authorities and the Heads of military investigating authorities at the regional command level or higher are empowered either on their own initiative or at the request of the Chief Procurator of the provincial-level People's Procuracy or the Chief Procurator of the military procuracy at the regional command level to issue decisions on the application of special investigative measures. In cases where a criminal case is being investigated by a district-level investigating authority or by a regional military investigating authority, the Head of the district-level investigating body or the Head of the regional military investigating body shall submit a proposal to the Head of the provincial-level investigating authority or the Head of the military investigating authority at the regional command level for consideration and decision. Any decision to apply special investigative measures must be approved by the Chief Procurator of the People's Procuracy of the same level before implementation. The Head of the investigating authority who has issued such a decision shall promptly request the Procuracy to cancel the measure if, upon review, it is deemed no longer necessary.

Accordingly, when the Head of an investigating authority with the requisite competence issues a decision to apply a special investigative measure, such a decision becomes effective only after it has been approved by the Chief Procurator of the People's Procuracy at the same level. However, the current law does not yet provide any explicit provision assigning the Chief Procurator the duty to supervise or monitor the execution of the approved measure once it is implemented. The above regulation also clarifies the distinction between those who are entitled to request and those who are entitled to propose the application of a special investigative measure. Specifically, the right to *request* the competent authority to issue a decision lies with the Chief Procurator of the provincial-level People's Procuracy and the Chief Procurator of the Military Procuracy at the regional command level (or equivalent). Meanwhile, the right to *propose* rests with the Heads of district-level investigating authorities and the Heads of regional military investigating authorities (or equivalent), who may submit such proposals to the competent authority for consideration and decision.

3.3.2. The duration of a special investigative measure refers to the minimum and maximum period prescribed by law during which such a measure may be conducted

Under the *CPC*, the period of application shall not exceed two months from the date on which the decision is approved by the Chief Procurator of the People's Procuracy. Special investigative measures may be applied only after the initiation of a criminal case and are to be conducted exclusively during the investigation stage. In complex cases requiring additional time to collect documents, evidence, or other relevant information, the duration of a special investigative measure may be

extended but must not exceed the overall statutory time limit for investigation. No later than ten days before the expiration of the authorized period, if an extension is deemed necessary, the Head of the investigating authority who issued the original decision must submit a written request to the Chief Procurator who granted approval, seeking consideration and decision on the extension.

3.3.3. Regarding the use of information and materials obtained through special investigative measures

According to Article 227 of the CPC, the information and materials gathered from the application of special investigative measures often involve elements of an individual's private life. Therefore, investigating authorities and persons conducting criminal proceedings must exercise the utmost caution in analyzing, evaluating, and selecting only those pieces of information and materials that possess evidentiary value in proving the offence. Such materials are to be used strictly within procedural boundaries to collect the necessary evidence for determining the perpetrator, identifying any accomplices, preventing flight or obstruction of justice, and tracing or recovering illicit assets acquired through criminal conduct.

The evidence obtained through special investigative measures during the investigation stage may be used subsequently as probative material in the prosecution and trial of a criminal case. To ensure that the privacy of individuals is not infringed, the process of screening, verifying, and evaluating this evidence must be conducted promptly, retaining only those materials directly relevant to the resolution of the case. Any information or materials unrelated to the case must be destroyed without delay, and it is strictly prohibited to use the collected data, materials, or evidence for any purpose other than the investigation and adjudication of the case.

Furthermore, under Clause 2 of Article 227 of the CPC, information and materials obtained through the application of special investigative measures may serve as admissible evidence in criminal proceedings. This constitutes an exceptionally important evidentiary source with direct probative value in proving the offence and determining criminal liability. To ensure the lawful and effective implementation and supervision of these measures, close coordination between the investigating authority and the People's Procuracy at the same level is required, allowing for an accurate assessment of whether the continued application of a special investigative measure remains necessary for resolving the case. Accordingly, Clause 3 of Article 227 stipulates that the investigating authority must immediately notify the Chief Procurator who approved the measure of the results obtained from its application.

3.3.4. Regarding the cancellation of the application of special investigative measures

Article 228 of the *CPC* provides for the cancellation of special investigative measures. During the course of applying such a measure, the Head of the investigating authority who issued the decision is required to conduct regular and rigorous supervision of its implementation. In cases where the continuation of the measure is no longer necessary, or where any violation occurs during its execution, the Head of the investigating authority must submit a written request to the Chief Procurator of the People's Procuracy at the same level, seeking cancellation of the measure.

For criminal cases investigated by district-level investigating authorities or regional military investigating bodies, any proposal to cancel a special investigative measure must first be submitted in writing to the provincial-level investigating authority or to the military investigating authority at the regional command level.

These higher-level bodies shall then forward a recommendation to the Procuracy of the same level for consideration and decision on cancellation.

The Chief Procurator who has approved the decision to apply a special investigative measure is obligated to revoke that decision without delay when any of the following circumstances arise: (1) a written request for cancellation is submitted by the competent Head of the investigating authority; (2) a violation has occurred in the process of implementing the measure; or (3) the continuation of the measure is deemed unnecessary.

The investigating authority bears the duty to promptly notify the Chief Procurator who granted approval of the results obtained from the application of the special investigative measure. Notably, with regard to measures such as covert audio and video recording, the *CPC* is the first legal instrument in Vietnam to formally recognize and authorize their use by investigating authorities. These are new and progressive techniques within the process of investigating and resolving criminal cases, carried out in secrecy both in terms of methods, subjects, and non-relevant information yet producing publicly admissible evidence of direct probative value. Such evidence serves to prove the offence, identify the perpetrator and accomplices, prevent escape or destruction of evidence, and trace or recover illicit assets for the purposes of investigation, prosecution, and adjudication.

Beyond the CPC's textual provisions, the practical operation of SIMs is structured by publicly issued coordination instruments that operationalize prosecutorial approval and supervisory routines. A key reference point is Joint Circular No. 04/2018/TTLT-VKSNDTC-BCA-BQP, which prescribes coordination between investigation bodies and the Procuracy in implementing a number of CPC provisions across initiation, investigation, and prosecution[49]. The Circular clarifies internal procedural steps relevant to SIMs, including communication duties, reporting lines, and supervisory interactions during the application period. It also specifies the institutional expectation that collected information and documents are handled in coordination with the Procuracy under the CPC's rules on use and processing of SIMs-derived materials[50]. Taken together, these implementing instructions do not "declassify" SIMs or make operational files publicly contestable; however, they are highly relevant to legal assessment because they reveal how the statutory model is intended to function as a system of internal checks, extensions, and cancellations within a secrecy-governed investigative domain.

3.3.5. Operational workflow and limits of visibility in practice

Publicly accessible materials indicate that SIMs in Vietnam are designed to operate through a tightly channeled workflow rather than open adversarial contestation. The CPC allocates decision-making and approval to senior investigative leadership and the chief procurator at the corresponding level, and the implementing Circular further details timelines and communication duties surrounding approval, extension, and cancellation.[51] This design has two implications for "Vietnamese practice" as observable from public sources. First, because SIMs are classified, published judgments and case summaries rarely disclose operational details; the absence of visible litigation narratives should

[49] SUPREME PEOPLE'S PROCURACY-MINISTRY OF PUBLIC SECURITY-MINISTRY OF NATIONAL DEFENSE. Joint Circular No. 04/2018/TTLT-VKSNDTC-BCA-BQP dated October 19, 2018, stipulates the coordination between the Investigation Agency and the People's Procuracy in implementing certain provisions of the Criminal Procedure Code. In., 2018. Available at: https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Thong-tu-lien-tich-04-2018-TTLT-BCA-BQP-TANDTC-VKSNDTC-phoi-hop-thuc-hien-tha-tu-truoc-thoi-han-364565.aspx (accessed on 26 May 2025).

[50] Ibid.

[51] Ibid.

therefore not be misread as the absence of rights-impacting surveillance practice. Second, what can be assessed through public materials is the safeguard architecture: whether legality thresholds are sufficiently specified, whether time limits and extension logic are controlled through reasoned decision-making, whether data-handling obligations are structured, and whether cancellation and accountability mechanisms are articulated as enforceable procedural constraints rather than discretionary options.

A central institutional feature of Vietnam's SIMs design is the allocation of both authorization (including approval/extension) and supervisory functions within the procuratorial channel. As a matter of legal architecture, this model concentrates legality control and compliance review in a single procedural actor, which can streamline coordination under secrecy but also narrows the space for demonstrable institutional separation and independent scrutiny. This allocation is therefore treated in this paper as the main institutional variable that shapes safeguard density in practice, and it serves as the baseline for the comparative assessment developed in Section 3.5.

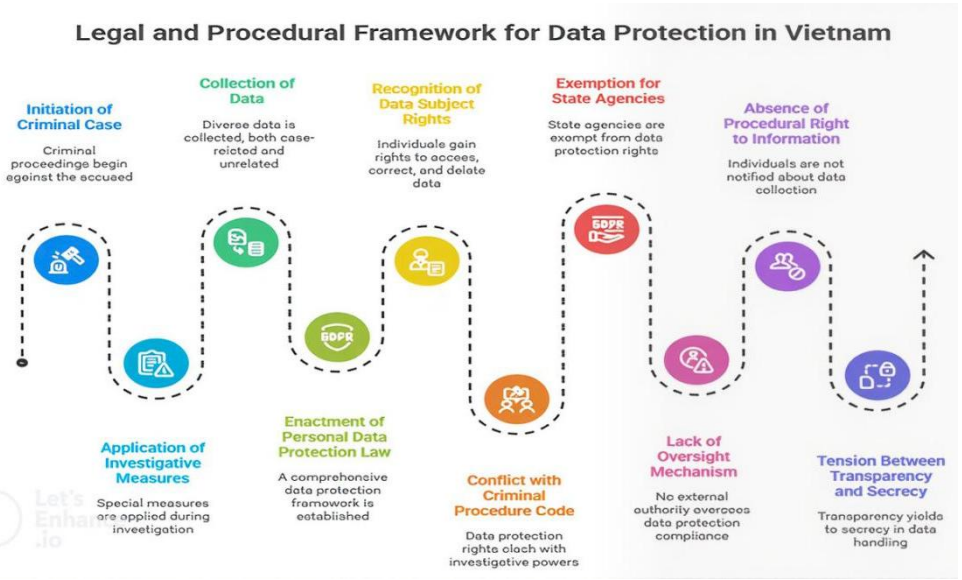

Figure 2. Legal and procedural framework for data protection in Vietnam.

3.4. Legal conflicts within Vietnam's regulatory framework on personal data and criminal investigation

Information and documents collected through SIMs are highly diverse and abundant. According to Article 227 of the CPC, such materials may be used for the initiation, investigation, prosecution, and adjudication of criminal cases. However, Article 223 stipulates that these measures may only be applied after a criminal case has been initiated and during the investigation phase. This inconsistency suggests that the issue lies not in the absence of legal provisions but in the ambiguity surrounding the scope and timing of SIMs' permissible application. While the law allows these measures "during the investigation of a criminal case," it simultaneously permits "the use of information and documents obtained therefrom for the initiation of criminal proceedings," implicitly allowing data collection even before a case is formally opened. This legislative gap creates the potential for ex post legalization of surveillance activities that intrude upon individual privacy, raising serious concerns about both the legality of such processes and the adequacy of privacy protections under Vietnamese criminal procedure. In practice, SIMs may be applied even before formal proceedings are initiated against a suspect, and the

collected materials may later be transformed into incriminating evidence. Yet, there are currently no clear provisions on the exclusion of such evidence, which may lead to its practical use[52]. Furthermore, any information or documents unrelated to the case must be promptly destroyed, and their use for other purposes is strictly prohibited. The law also lacks clarity on whether information obtained during SIMs for one case can be used to initiate proceedings in another case under Article 143 of the CPC, thereby raising further concerns about potential violations of citizens' right to information privacy.

The CPC does impose an important safeguard: information and documents unrelated to the case must be promptly destroyed, and their use for other purposes is prohibited. However, the Code does not clearly address whether SIM-derived information gathered in one case may be relied upon to trigger proceedings in another context (for example, under Article 143 on the initiation of criminal cases), nor does it articulate sufficiently detailed procedural constraints for such cross-context reliance. This gap is not merely technical. In secrecy-governed measures, data flows are difficult to observe from the outside, so unclear rules on scope, timing, reuse, and evidentiary consequences can translate into structurally weak privacy protection even where "legality" is formally asserted.

Against this procedural backdrop, Vietnam's Personal Data Protection Law 2025 (Law No. 91/2025/QH15) introduces an explicitly rights-facing data-governance framework. At the level of principle, Article 4 enumerates the rights of data subjects, including the entitlement to request the provision of data, deletion, and restriction of processing. Article 14 operationalises deletion through specific grounds and duties most notably where the processing purpose has been fulfilled, where statutory retention periods expire, or where deletion follows a competent authority's decision. On paper, this structure resonates with the normative intuition behind the GDPR's "right to erasure" (Article 17): personal data should not be retained beyond a lawful and necessary purpose. Yet the statute simultaneously embeds a critical limitation that is particularly salient for secrecy-governed domains. Article 14(2) permits refusal of deletion requests where the processing falls within Article 19 (processing without the data subject's consent). As a matter of legal design, the question is therefore not whether Vietnam recognises an erasure norm, but whether the surrounding limitation structure allows the right to remain meaningfully justiciable in contexts most associated with coercive state data collection.

This is where the PDPL's rights vocabulary collides with the operational logic of SIMs. Deletion is framed as a rights-facing entitlement, but its practical invocation presupposes procedural visibility: the data subject must be able to identify that processing occurred, locate the controller holding the data, and access a contestable pathway to review refusals particularly where refusals are grounded in non-consensual processing. In covert investigative settings, individuals are typically not notified while measures are ongoing, and post-operation disclosure is not structured as a routine procedural entitlement once secrecy is no longer necessary. The result is an enforceability gap: the right exists in principle, but the conditions that trigger and sustain the right are systematically weakened in the very environments where state data collection is most privacy-intrusive.

Finally, the enforceability of data-subject rights is shaped by institutional design. The PDPL assigns specialised personal-data protection functions within a system led by the Ministry of Public Security, which is also central to law-enforcement functions in criminal procedure. This configuration does not negate data protection as a doctrinal commitment, but it tends to place rights-enforcement closer to internal

[52] THUYEN, T. D. (2025). "Fruit of the Poison Tree Doctrine in US Criminal Proceedings and Regulations on the Exclusion of Evidence in Vietnamese Criminal Proceedings". International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique, 38(2), 443-461.

administrative control than to demonstrably independent, rights-facing scrutiny especially in secrecy-governed investigative contexts. In my assessment, the core normative imbalance is therefore structural: Vietnam's PDPL articulates a transparency-oriented language of rights, while SIMs operate through secrecy. When these regimes intersect, the decisive variable is not the existence of the "right to erasure" on paper, but whether procedural architecture visibility, contestability, and review renders that right operational as a constraint on state data power.

3.5. Comparative analysis: The Vietnamese legal framework and European human rights standards on special investigative measures

The regulation of SIMs in Vietnam's CPC represents a significant legislative step towards transparency and modernization. Yet, when viewed through the lens of international human rights law particularly the *ECHR*, the *ICCPR* and the jurisprudence of the *ECtHR,* the Vietnamese framework reveals clear normative gaps. These gaps do not necessarily stem from legislative neglect but from structural differences in the conception of legality and accountability. While European law builds its legitimacy on judicial control and individual rights, Vietnam's system still rests heavily on prosecutorial authority and institutional coordination.

To facilitate a systematic comparison, eight benchmark criteria are derived from international human rights instruments and European jurisprudence (Table 1). They serve as a normative compass to assess how far the Vietnamese framework aligns with global standards and where it diverges in protecting the right to privacy and due process.

Justification and operationalization of the comparative criteria. The eight criteria are not an ad hoc checklist; they are derived from the European legality legitimate aim–necessity/proportionality framework under Article 8 ECHR, as refined in ECtHR case law on secret surveillance, and complemented by data-governance requirements developed in EU law for law-enforcement processing (including purpose limitation, data minimization, storage limitation, and supervised erasure). Taken together, the criteria cover the full "lifecycle" of SIMs:

(i) ex ante authorization standards (legality, necessity, proportionality, independent oversight).

(ii) Implementation and data handling (data protection and destruction).

(iii) Ex post accountability (post-notification/transparency, fair-trial safeguards on evidentiary use, and effective remedies).

This lifecycle approach allows the CPC rules to be evaluated not only for formal legality, but for the density and independence of safeguards that prevent arbitrariness and enable meaningful accountability.

Table 1. Comparative Assessment of Special Investigative Measures: Vietnamese CPC vs. European Human Rights Standards.

Criterion	**European Human Rights Standard (ECHR / EU Law)**	**Vietnamese Legal Framework (CPC)**	**Critical Assessment**
Legality	Surveillance must be clearly defined by accessible and foreseeable laws (ECHR Art. 8; *Klass v. Germany*, 1978; *Zakharov v. Russia*, 2015).	Chapter XVI (Arts. 223–228 the CPC) defines SIMs and their conditions, but lacks detailed procedural safeguards and definitions of "particularly serious crimes."	The Vietnamese provisions establish legality in form but not in precision. Vague definitions grant broad discretion, weakening predictability and increasing the risk of arbitrary interpretation.

Criterion	**European Human Rights Standard (ECHR / EU Law)**	**Vietnamese Legal Framework (CPC)**	**Critical Assessment**
Necessity	Measures may be applied only when ordinary investigative means are ineffective and for legitimate aims (*Weber & Saravia v. Germany*, 2006).	SIMs can be applied only after a case is initiated, but there is no explicit requirement to prove the insufficiency of conventional methods before approval.	The absence of a necessity test reduces the normative threshold; measures may be authorized based on administrative convenience rather than compelling justification.
Proportionality	Intrusion must be proportionate to the public interest served; excessive or indiscriminate surveillance violates Art. 8 ECHR (*Big Brother Watch v. UK*, 2021).	CPC limits duration to two months (extendable within investigation period), but lacks guidance on assessing proportionality between the degree of intrusion and investigative value.	The Vietnamese framework focuses on time limits rather than substantive proportionality. There is no balancing test to weigh privacy intrusion against investigative gain.
Independent Oversight	Judicial authorization and supervision by independent courts (*Szabó & Vissy v. Hungary*, 2016).	Authorization and oversight are conducted by the People's Procuracy, which also exercises prosecutorial powers.	Oversight lacks independence. Combining prosecutorial and supervisory roles creates potential bias and conflicts of interest.
Data Protection and Destruction	GDPR Art. 5 & 17: principles of data minimization, storage limitation, and right to erasure; *Zakharov v. Russia* requires prompt deletion of irrelevant data.	Art. 227 CPC requires destruction of irrelevant materials but lacks a detailed protocol, external audit, or sanction for breaches.	While commendable in intent, the absence of procedural detail and sanctions renders data protection largely symbolic.
Transparency and Post-Notification	Individuals must be notified after surveillance when secrecy is no longer required (*Klass v. Germany*, *Zakharov v. Russia*).	Vietnamese law is silent on post-investigation notification and offers no mechanism for complaint or compensation.	The lack of post-fact transparency denies individuals the right to know and seek remedies contrary to ECHR standards.
Admissibility and Fair Trial	Evidence obtained through entrapment or unlawful surveillance is inadmissible (*Teixeira de Castro v. Portugal*, 1998).	Art. 227(2) CPC allows use of information from SIMs as evidence without clear criteria for legality or exclusion of unlawfully obtained material.	There is no exclusionary rule to protect fair trial rights; this gap risks legitimizing tainted evidence.
Remedies and Accountability	Art. 13 ECHR & Art. 2(3) ICCPR guarantee an effective remedy and compensation for rights violations.	No explicit remedies for unlawful surveillance; disciplinary action depends on internal administrative review.	The absence of a judicial or civil remedy mechanism leaves individuals unprotected and weakens institutional accountability.

Note: "European standard" is synthesized from Article 8 ECHR, relevant ECtHR case law, and (where applicable) EU data-protection instruments used as persuasive guidance for law-enforcement data governance. Sources: European Convention on Human Rights, Arts. 8 and 13; ICCPR Art. 2(3); Directive (EU) 2016/680; Vietnamese's CPC, Chapter XVI (Arts. 223–228).

As shown in the comparative table above, Vietnam's CPC provides a formal legal basis for SIMs, yet the safeguard architecture is less fully specified than the European model across four interrelated dimensions. First, legality in the CPC is expressed primarily through statutory authorization, whereas European standards require legality in a substantive sense clear scope, foreseeable thresholds, and sufficiently detailed safeguards, including supervision modalities. Second, the CPC does not expressly structure necessity and proportionality as mandatory decision tests at the authorization stage; in European jurisprudence, these operate as substantive constraints that require a reasoned showing of necessity and consideration of less intrusive alternatives. Third, the CPC's authorization and supervisory design relies predominantly on internal procedural control within prosecution-led procedural channels, while the European model places greater weight on prior independent authorization and continuing independent review. Fourth, ex post accountability remains under-specified: the CPC does not establish a systematic post-notification mechanism, and the remedial pathway for unlawful surveillance is not articulated as a clearly enforceable procedural entitlement. Taken together, these doctrinal and procedural divergences help explain how a framework may achieve formal codification without fully embedding the safeguard density typically associated with contemporary privacy and data-protection standards.

The strongest innovation of Vietnam's system lies in its legal codification of secrecy. By embedding special investigative measures (such as surveillance, wiretapping, and data interception) into statutory law, the State has replaced informal police discretion with procedural legality an undeniably positive move that aligns with the United Nations Convention against Corruption and the Convention against Transnational Organized Crime. Yet this reform primarily ensures *vertical control* (within institutions) rather than *horizontal accountability* (between the State and the citizen). The Procuracy supervises investigators, but no independent judicial or civilian body supervises the Procuracy itself. The absence of prior judicial authorization remains the most serious shortcoming: unlike in the European Union, where even national security surveillance typically requires pre-approval from an independent judge or specialized court, in Vietnam both authorization and cancellation rest with the Procuracy the same body that directs prosecution. This duality undermines the impartiality principle embedded in Article 8 of the ECHRand Article 17 of the ICCPR (UN Human Rights Committee, General Comment No. 16, 1988). Moreover, the lack of a proportionality test an essential safeguard in European jurisprudence means that privacy intrusions are measured by duration rather than necessity. Without a normative yardstick linking the degree of intrusion to the gravity of the offence, the boundary between what is "necessary" and what is merely "convenient" becomes dangerously blurred. Ultimately, Vietnam's progress in procedural codification is commendable, but its failure to incorporate judicial oversight and proportionality reasoning continues to limit the human-rights compatibility of its criminal procedure.

The SIMs as provided for in the current The Vietnam's CPC, remain a subject of divergent views regarding their application. Proponents argue that, in practice, investigative authorities have already employed certain professional techniques in addressing particularly serious offenses, organized crime, and complex cases. Codifying these measures is deemed necessary to ensure conformity with the constitutional principle that "human rights and citizens' rights may only be restricted by law,"[53] while also providing a legal foundation for the implementation of international treaties to which Vietnam is a party. The formal regulation of SIMs would help overcome practical challenges in crime prevention and facilitate the collection of sufficient, legally admissible evidence to directly establish criminal liability. Critics argue that the potential misuse of special investigative measures

[53] TUYEN, P. M. (2019). Ibid.

could violate human rights and civil liberties, thereby fostering public apprehension and undermining citizens' sense of security.[54] Many opinions suggest that there must be clear and specific guidance on the subjects, circumstances, and contexts in which special investigative measures should be applied[55]. If used indiscriminately, such measures may infringe upon individuals' right to privacy. Given the brevity of statutory provisions, responsible authorities must promptly issue detailed implementation guidelines, as this is a newly introduced legal mechanism. The Procuracy should strengthen its oversight of the application of these measures; likewise, courts must examine whether the evidence presented in a case has been collected in accordance with legal procedures. Ultimately, the role of those directly involved remains the most critical. Investigators and prosecutors must assess each specific case to propose the application of such measures, and those in charge must carefully consider and address these proposals

The data-protection framework under Article 227 CPC demonstrates Vietnam's awareness of privacy risks, yet the regulation remains procedural rather than substantive. Unlike the GDPR, it does not specify retention periods, access rights, or penalties for unlawful disclosure. In practice, once surveillance data enter institutional archives, their lifecycle is governed more by administrative habit than by legal precision. This situation risks transforming evidentiary data into bureaucratic information rather than treating them as sensitive personal material deserving constitutional care. This structural tension is summarized in Figure below, which conceptualizes Vietnam's current legal and privacy framework governing the SIMs. The figure illustrates how the codification of secrecy and vertical institutional control have been achieved procedurally, yet the absence of horizontal accountability, proportionality testing, and prior judicial authorization continues to undermine the protection of individual privacy under the Criminal Procedure Code.

Equally significant is the absence of post-notification and remedies. In Europe, individuals have the right to be informed once secrecy is no longer required, and to challenge the legality of surveillance before courts or data protection authorities. In Vietnam, surveillance ends where secrecy ends no one outside the system ever learns it occurred. This silence may preserve operational efficiency, but it corrodes public trust and violates the principle of transparency that sustains democratic legitimacy.

Finally, the admissibility of evidence collected through SIMs raises both evidentiary and moral questions. The CPC recognizes such information as lawful evidence without requiring proof of legality in acquisition. In contrast, the ECtHR's case law such as *Teixeira de Castro v. Portugal* excludes evidence obtained through entrapment or manipulation. By lacking an exclusionary rule, the Vietnamese framework risks rewarding procedural shortcuts and undermining the fairness of trials protected under Article 31 of the Constitution and Article 6 ECHR.

In sum, the comparative picture suggests that Vietnam's system is legalistic but not yet humanistic. It emphasizes institutional order rather than individual rights, procedural correctness rather than proportional justice. The European model, though not flawless, offers a more holistic vision in which legality, necessity, proportionality, and accountability function as interconnected safeguards. If Vietnam seeks to align its criminal procedure with international human rights standards, the next phase of reform should focus not on expanding investigative power but on perfecting its constraints. Only by doing so can the law achieve what

---

[54] HAI, P. L. (2024). "Special Procedural Investigative Measures – Provisions under the 2015 Criminal Procedure Code, Challenges and Recommendations". People's Court Journal, (20). Available at: https://tapchitoaan.vn/bien-phap-dieu-tra-to-tung-dac-biet-quy-dinh-cua-bo-luat-to-tung-hinh-su-nam-2015-vuong-mac-va-kien-nghi12969.html (accessed on 26 May 2025).

[55] DUY, L. H. T. 2023. Ibid.

Montesquieu once called *"the gentle power of moderation"* a justice strong enough to act, yet humble enough to restrain itself.

Figure 3. Conceptual map of Vietnam's legal and privacy framework on SIMs.

On this basis, Section 3.6 translates the comparative gaps into institutionally feasible reform directions for Vietnam, focusing on authorization design, data governance, post-notification, and remedies.

3.6. Policy implications and reform directions

3.6.1. Institutional feasibility and sequencing of reforms

The comparative analysis above suggests that Vietnam's core challenge lies less in the absence of legal norms than in how those norms operate within existing institutional and procedural allocations. Although the CPC has codified the SIMs under the principle of legality, a persistent gap remains between public-order imperatives and rights-facing safeguards particularly in contexts where secrecy limits transparency and contestability. Bridging this gap requires reforms that are both normatively grounded and institutionally feasible.

Introducing prior independent judicial authorization for SIMs faces identifiable obstacles within Vietnam's current procedural architecture. First, the CPC's design embeds prosecutorial approval as the principal legality checkpoint; moving toward judicial authorization would therefore require not only statutory amendment but also secure handling protocols for classified materials, calibrated timelines for urgent measures, and standardized reasoning templates capable of demonstrating necessity and proportionality. Second, an authorization-court model presupposes capacity and infrastructure trained judges, secure facilities, sealed record-keeping, and specialised procedures to ensure that independent review is operationally workable in a secrecy-governed domain. Third, because SIMs are routinely justified by urgency and investigative efficiency, reform choices must avoid procedural bottlenecks, for example by differentiating between routine approvals and higher-risk measures or longer extensions.

Institutional resistance is most plausibly framed as a mandate-and-efficiency concern rather than a principled rejection of rights protection. Where authorization and supervisory functions are currently administered within a procuratorial channel, additional independent review may be perceived as diluting coordination speed, increasing exposure to procedural challenges, and heightening accountability risks for operational decisions. Reform should therefore be articulated as legality-strengthening and risk-management rather than authority displacement by focusing

on safeguards that protect legitimate investigative objectives while reducing arbitrariness and improving reason-giving and reviewability.

Accordingly, reform is best conceptualised as a sequenced safeguard upgrade rather than a single institutional leap. An initial package should prioritise enforceable ex post constraints structured post-operation review, retention-and-erasure auditing, mandatory logging and sealed documentation, and a limited post-notification mechanism subject to narrowly defined postponement grounds because these measures strengthen accountability without immediately re-engineering the authorization model. Once these mechanisms produce stable practice and demonstrable compliance, a second step can introduce targeted independent review for higher-risk scenarios, such as judicial validation for extensions beyond a defined duration or for the most intrusive measures, while routine approvals remain within the existing channel. Only after capacity, secure procedures, and consistency in proportionality reasoning are established should the system transition toward fuller ex ante judicial authorization. In this staged design, feasibility is not treated as a political constraint but as a functional condition for rights protection: reforms that can be implemented, audited, and reviewed are more likely to generate lasting safeguards than reforms that are normatively attractive but institutionally brittle.

3.6.2. Legislative clarification of the temporal scope and evidentiary limits of SIMs

The inconsistency between Articles 223 and 227 of the CPC reveals a structural defect that undermines both the principle of legality and the protection of individual privacy. Article 223 stipulates that SIMs may only be applied after the initiation of a criminal case and during the investigative stage, thereby establishing a temporal safeguard intended to prevent arbitrary interference. However, Clause 1 of Article 227 simultaneously authorizes the use of information and documents collected through such measures for the *initiation, investigation, prosecution, and adjudication* of criminal cases. At first glance, this overlap may appear merely technical, but in substance it creates a legal vacuum that allows surveillance data gathered prior to the initiation of criminal proceedings to be subsequently "regularized" and admitted as evidence. In other words, what was designed as a preventive mechanism has been transformed into a permissive one. From my standpoint, this inconsistency cannot be resolved through interpretive techniques alone but requires legislative clarification. Article 223 should be amended to affirm explicitly that *special investigative measures may only be applied after a formal decision to initiate criminal proceedings pursuant to Article 143 of the CPC*. An additional clause could provide that: *"Any information or document obtained prior to the initiation of criminal proceedings shall have no evidentiary value and may be used solely for operational reference."* Such a concise amendment would eliminate the risk of legitimizing evidence collected at an improper stage and would bring Vietnam's procedural framework closer to international standards of legality and necessity in criminal justice.

3.6.3. Strengthening data governance, oversight, and post-operation accountability

From the comparative analysis above, it is apparent that Vietnam's challenge does not stem from a lack of legal provisions but from the structure of its control and accountability mechanisms. The delegation of authority to approve the SIMs to the People's Procuracy at the provincial level represents a systemic choice rooted in Vietnam's legal tradition one in which legality is safeguarded primarily through hierarchical supervision rather than through independent judicial oversight. Although this model differs from the European approach, which relies on judicial

authorization, it is not necessarily inconsistent with international human rights standards. The central issue is not who grants authorization, but rather how the process is supervised, monitored during implementation, and reviewed after completion. In other words, the legitimacy of covert surveillance does not arise solely at the moment of approval; it depends on the system's continuing capacity to prevent abuse, correct irregularities, and ensure effective remedies.

Accordingly, the most urgent reform should focus on clarifying the procedures for processing, storing, and destroying data obtained through SIMs once that data no longer possesses evidentiary value. Article 227 of the current the CPC provides only a brief reference to the destruction of "irrelevant materials," without defining who determines such irrelevance, within what time frame, or under what verification mechanism. This ambiguity may unintentionally transform "secrecy" into a space for discretion. To remedy this, a Joint Circular should be promulgated by the Supreme People's Procuracy, the Ministry of Public Security, and the Ministry of Justice, establishing a clear procedural chain:

(i) the investigating authority shall compile a comprehensive inventory of all data collected through SIMs;

(ii) the Procuracy shall review the necessity of data retention within fifteen days after the conclusion of the measure;

(iii) the Procuracy shall order the deletion, anonymization, or secure storage of non-relevant data under the supervision of an inter-agency audit committee.

Once institutionalized, this process would ensure that secrecy serves justice rather than conceals it. Another crucial issue lies in the interaction between the CPC and the Law on Personal Data Protection (2025). The latter establishes general principles of lawfulness, purpose limitation, and data minimization but does not yet specify their application in criminal investigations. The solution is not to amend the law itself, but to issue interpretive and procedural guidance ensuring consistency with Vietnam's international obligations under the ICCPR. A Joint Resolution between the Supreme People's Court and the Supreme People's Procuracy could affirm that personal data collected through SIMs shall be used exclusively for evidentiary purposes in the specific case concerned, and that any secondary use for intelligence, disciplinary, or administrative purposes must be strictly prohibited. This interpretive harmonization would bring Vietnam closer to the principles of necessity and proportionality developed in the jurisprudence of the ECtHR without mechanically transplanting a foreign judicial model.

Furthermore, post-operation accountability must be strengthened. Under the current system, ex post review by the Procuracy is the only safeguard, and individuals are not entitled to learn even after the conclusion of a case that they were subject to surveillance. It would therefore be advisable to introduce a limited post-notification mechanism, allowing the Procuracy to inform affected persons once disclosure no longer endangers national security or ongoing investigations. Even a modest level of transparency would significantly enhance public trust and help realize the constitutional commitment that human rights may be restricted only by law.

Ultimately, the objective is not to replicate the European system but to humanize Vietnam's own procedural tradition. The Procuracy-based authorization mechanism may well be preserved, yet it should be bound by substantive standards of necessity, proportionality, and personal data protection at every stage from authorization and implementation to data destruction. As Montesquieu observed, "liberty does not consist in the absence of power, but in the limitation of its use." Vietnam's legal framework has already made a decisive step by codifying secrecy; the next step must ensure that secrecy becomes accountable and humane.

4. Conclusion

From the foregoing analysis and policy recommendations, it is evident that Vietnam has made significant progress in codifying SIMs within its CPC, marking a crucial step toward greater transparency and accountability in criminal justice. Yet, the primary challenge no longer lies in the absence of legal provisions, but rather in ensuring their effective implementation and enforceability in practice. The coordination among procedural authorities must be firmly grounded in the principles of personal data protection, necessity, and proportionality, while preserving the institutional characteristics of Vietnam's prosecutorial oversight model.

In the broader context of global legal integration, Vietnam does not need to replicate the European Union's judicial framework. Instead, it should internalize the human rights spirit through mechanisms compatible with its institutional structure. The essence of reform lies in transforming "secrecy" into accountable confidentiality a system in which every act of data collection, processing, or destruction is subject to verifiable oversight, traceability, and independent evaluation. If achieved, Vietnam's criminal justice system will not only strengthen its capacity to combat and prevent crime but will also embody the values of a modern, humane, and rights-respecting judiciary, consistent with the 2013 Constitution and Vietnam's international human rights commitments.

5. Declaration

The author declares that artificial intelligence (AI) tools were used solely to assist with language editing, including checking grammar, spelling, and improving clarity and readability of the manuscript. The use of AI was limited to technical proofreading and did not replace the author's scholarly judgment, research design, data analysis, or scientific conclusions. The author affirms that all ideas, arguments, structure, data, interpretations, and the full academic content of this article were independently developed and written by the author, who takes complete responsibility for the accuracy, integrity, and originality of the work.

6. Funding

This paper is a product of a university-level research project code: CELG-CS-2025-10 funded by the University of Economics Ho Chi Minh City, Vietnam (UEH).

7. References

ASSEMBLY, U. G. (1948). "Universal declaration of human rights". UN General Assembly, 302(2), 14-25.

BROWNSWORD, R. "Law, Technology and Society: Reimagining the Regulatory Environment". (1st ed.) Edtion ed.: Routledge, 2019.

CHANH, P. V. (2018). "Special investigative procedural measures in Vietnam's criminal proceedings". Journal of People's Procuracy of Vietnam, 11. Available at: https://tlpl.moj.gov.vn/Pages/chi-tiet-bai-trich.aspx?ItemID=1506&CategoryBTTC=BTTC (accessed on 26 October 2025).

COURT OF JUSTICE OF THE EUROPEAN UNION. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources (Joined Cases C-293/12 and C-594/12). EUR-Lex. In., 2014. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293 (accessed on 26 October 2025).

COURT OF JUSTICE OF THE EUROPEAN UNION. La Quadrature du Net and Others v. France (Joined Cases C-511/18, C-512/18, and C-520/18). In., 2020. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CA0511 (accessed on 26 October 2025).

COURT OF JUSTICE OF THE EUROPEAN UNION. Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others (Joined Cases C-

203/15 and C-698/15). EUR-Lex / CURIA. In., 2016. Available at: https://curia.europa.eu/juris/liste.jsf?num=c-203/15 (accessed on 26 October 2025).
DAHL, J. Y. (2022). "Chameleonizing: A microsociological study of covert physical surveillance". European Journal of Criminology, 19(2), 220-236.
DIRECTIVE (EU). Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. In., 2016. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680 (accessed on 26 October 2025).
DUY, L. H. T. (2023). "Comparative research on special investigation measures and experiences for Vietnam". Procuratorate Studies, 03. Available at: https://vjol.info.vn/index.php/tks/article/view/82153 (accessed on 26 October 2025).
ESEN, R. (2012). "Intercepting Communications 'In Accordance with the Law'". The Journal of Criminal Law, 76(2), 164-178.
EUROPE, C. O. European Convention on Human Rights, [online]. 1950. Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG (accessed on 26 October 2025).
EUROPEAN COURT OF HUMAN RIGHTS. (2025). "Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life". ECHR Knowledge Sharing (ECHR-KS).
EUROPEAN COURT OF HUMAN RIGHTS. Case of Klass and others v. Germany (Application no. 029/71).HUDOC. In.: European Court Of Human Rights, 1978. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]} (accessed on 26 May 2025).
EUROPEAN COURT OF HUMAN RIGHTS. Roman Zakharov v. Russia (Application no. 47143/06). Strasbourg: ECtHR.HUDOC. In., 2015. Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22] (accessed on 26 October 2025).
GENERAL ASSEMBLY RESOLUTION. The International Covenant on Civil and Political Rights [online]. 1966. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (accessed on 26 October 2025).
GENERAL DATA PROTECTION REGULATION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC In., 2016. EUROPE, C. O. European Convention on Human Rights, [online]. 1950. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 26 October 2025).
HAI, P. L. (2024). "Special Procedural Investigative Measures – Provisions under the 2015 Criminal Procedure Code, Challenges and Recommendations". People's Court Journal, (20). Available at: https://tapchitoaan.vn/bien-phap-dieu-tra-to-tung-dac-biet-quy-dinh-cua-bo-luat-to-tung-hinh-su-nam-2015-vuong-mac-va-kien-nghi12969.html (accessed on 26 May 2025).
HILDEBRANDT, M. "Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology". In Smart Technologies and the End (s) of Law: Edward Elgar EBooks, 2016.
HILL, D. J., S. K. MCLEOD AND A. TANYI. (2024). "Policing, undercover policing and 'dirty hands': the case of state entrapment". Philosophical Studies, 181(4), 689-714.
HO, H. L. (2011). "State entrapment". Legal Studies, 31(1), 71-95.
KOMUKAI, T. "Privacy Protection During Criminal Investigations of Personal Data Held by Third Parties". In IFIP International Conference on Human Choice and Computers. Cham: Springer International Publishing, 2022, p. 200-212.
KRUISBERGEN, E. W., D. DE JONG AND E. R. KLEEMANS. (2011). "Undercover Policing: Assumptions and Empirical Evidence". The British Journal of Criminology, 51(2), 394-412.
LOFTUS, B. AND B. GOOLD. (2012). "Covert surveillance and the invisibilities of policing". Criminology & Criminal Justice, 12(3), 275-288.
MATAR, R. AND D. MURRAY. (2025). "Re-thinking international human rights law's approach to identity in light of surveillance and AI". Human Rights Law Review, 25(3), ngaf016.

MURPHY, B. AND J. ANDERSON. (2016). "Confessions to Mr Big:A new rule of evidence?". The International Journal of Evidence & Proof, 20(1), 29-48.

NATIONAL ASSEMBLY. Criminal Procedure Code. In., 2015. Available at: https://thuvienphapluat.vn/van-ban/Thu-tuc-To-tung/Van-ban-hop-nhat-46-VBHN-VPQH-2025-Bo-Luat-To-tung-hinh-su-647146.aspx (accessed on 26 October 2025).

ORMEROD, D. AND A. ROBERTS. (2002). "The Trouble with Teixeira: Developing a Principled Approach to Entrapment". The International Journal of Evidence & Proof, 6(1), 38-61.

PHUOC, N. S. (2022). "Assessment of provisions on special investigative measures in the 2015 criminal procedure code and recommendation for complete". Journal of Science and Technology, 5(3). Available at: https://doi.org/10.56097/binhduonguniversityjournalofscienceandtechnology.v5i3.56 (accessed on 26 May 2025).

PRIYANKA, S. AND SWEKSHA. (2024). "Role of Right to Privacy in the Criminal Justice System". International Journal for Multidisciplinary Research, 6(3), 1-16.

PRYSIAZHNIUK, I. (2023). "Use of Digital Evidence in Criminal Process: Some Issues of Right to Privacy Protection". Visegrad Journal on Human Rights, 5, 81-88.

RESOLUTION, G. A. (1966). "International covenant on economic, social and cultural rights". General Assembly Resolution A.

SOLOVE, D. J. (2002). "Conceptualizing Privacy". California Law Review, 90(4), 1087-1155.

STEVENS, A., FUSSEY P., MURRAY, D., HOVE, K., SAKI, O. (2023). "'I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe". Big Data & Society, 10(1), 20539517231158631.

SUPREME PEOPLE'S PROCURACY-MINISTRY OF PUBLIC SECURITY-MINISTRY OF NATIONAL DEFENSE. Joint Circular No. 04/2018/TTLT-VKSNDTC-BCA-BQP dated October 19, 2018, stipulates the coordination between the Investigation Agency and the People's Procuracy in implementing certain provisions of the Criminal Procedure Code. In., 2018. Available at: https://thuvienphapluat.vn/van-ban/Trach-nhiem-hinh-su/Thong-tu-lien-tich-04-2018-TTLT-BCA-BQP-TANDTC-VKSNDTC-phoi-hop-thuc-hien-tha-tu-truoc-thoi-han-364565.aspx (accessed on 26 May 2025).

TAYLOR, C. (2005). "Entrapment: Abuse of Process:R v Lewis (Michael William) [2005] EWCA Crim 859". The Journal of Criminal Law, 69(5), 380-384.

THE HUMAN RIGHTS COMMITTEE. CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. In., 1988. Available at: https://www.refworld.org/legal/general/hrc/1988/en/27539 (accessed on 26 May 2025).

THUYEN, T. D. (2025). "Fruit of the Poison Tree Doctrine in US Criminal Proceedings and Regulations on the Exclusion of Evidence in Vietnamese Criminal Proceedings". International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique, 38(2), 443-461.

TURANJANIN, V. (2022). "Special investigative measures: Comparison of the Serbian Criminal Procedure Code with the European Court of Human Rights Standards". The International Journal of Evidence & Proof, 26, 34-60.

TUYEN, P. M. (2019). "Reflections on Special Investigative Procedures under the 2015 Criminal Procedure Code". Procuratorate Studies, 06. Available at: https://vjol.info.vn/index.php/tks/article/download/46430/37679/ (accessed on 26 October 2025).

VERVAELE, J. A. (2009). "Special procedural measures and the protection of human rights General report". Utrecht Law Review, 5(2).

WARREN, S. D., BRANDEIS, L. D. (1890). "The Right to Privacy". Harvard Law Review, 4(5).